Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 8(6): 12793–12818.
DOI:10.3934/math.2023644
Received: 18 September 2022
Revised: 25 October 2022
Accepted: 01 November 2022
Published: 30 March 2023

Research article

Repeated-root constacyclic codes of length $p_1 p_2^t p^s$ and their dual codes

Hongfeng Wu[1] **and Li Zhu**[2,*]

[1] College of Science, North China University of technology, Beijing 100144, China
[2] School of Mathematics and Statistics, Guizhou University, Guiyang 550025, China

* **Correspondence:** Email: mathcurve@163.com.

Abstract: Let $\mathbb{F}_q$ be the finite field with $q = p^k$ elements, and p_1, p_2 be two distinct prime numbers different from p. In this paper, we first calculate all the q-cyclotomic cosets modulo $p_1 p_2^t$ as a preparation for the following parts. Then we give the explicit generator polynomials of all the constacyclic codes of length $p_1 p_2^t p^s$ over $\mathbb{F}_q$ and their dual codes. In the rest of this paper, we determine all self-dual cyclic codes of length $p_1 p_2^t p^s$ and their enumeration. This answers a question recently asked by B. Chen, H.Q.Dinh and Liu. In the last section, we calculate the case of length $5\ell p^s$ as an example.

Keywords: finite fields; cyclic codes; constacyclic codes; cyclotomic cosets; dual code
Mathematics Subject Classification: 11T71, 12Y05, 94B15

1. Introduction

As a generalization of cyclic codes and negacyclic codes, constacyclic codes were first introduced by Berlekamp in 1968 [3]. Given a nonzero element λ in a finite filed $\mathbb{F}_q$, a linear code C of length n over $\mathbb{F}_q$ is called λ-constacyclic if $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C$ for every $(c_0, c_1, \cdots, c_{n-1}) \in C$. Constacyclic codes over finite fields form a remarkable class of linear codes, as it includes the class of cyclic codes and the class of negacyclic codes as proper subclasses. Constacyclic codes have rich algebraic structure so that they can be efficiently encoded and decoded by means of shift registers. Repeated-root constacyclic codes were a special class of constacyclic codes. Repeated-root constacyclic codes were first studied by Castagnoli et al. [4] and van Lint [13], and they showed that repeated-root cyclic codes have a concatenated construction and are not asymptotically good.

Recently, repeated-root constacyclic codes have been studied by many authors. To determine the generator polynomials of all constacyclic codes of arbitrary length over finite fields is an important problem. Dinh studied repeated-root constacyclic codes of lengths $2p^s$, $3p^s$, $4p^s$ and $6p^s$ in a series of papers [8–11]. He determined the algebraic structure of these repeated-root constacyclic codes over finite fields in terms of their generator polynomials. In [7], Chen et al. introduced an equivalence relation called isometry for the nonzero elements of $\mathbb{F}_q$ to classify constacyclic codes of length n over $\mathbb{F}_q$. They have the same distance structures and the same algebraic structures for belonging to the same equivalence classes induced by isometry. Furthermore, in [5], Chen et al. considered a more specified relationship than isometry that enabled us to obtain more explicit description of generator polynomials of all constacyclic codes. According to the equivalence classes, all constacyclic codes of length ℓp^s over $\mathbb{F}_{q^m}$ and their dual are characterized, where ℓ is a prime different from p and s is a positive integer. In 2012, Bakshi and Raka [1] also determined all Λ-constacyclic codes of length $2^t p^s (t \geq 1, s \geq 0$ are integers) over $\mathbb{F}_{p^r}$ using different methods from Chen et al.. In 2015, Chen et al. [6] determined the algebraic structure of all constacyclic codes of length $2\ell^m p^s$ over $\mathbb{F}_{p^r}$ and their dual codes in terms of their generator polynomials, where ℓ, p are distinct odd primes and s, m are positive integers. In the conclusion of the paper [6], they proposed an open problem to study all constacyclic codes of length $k\ell^m p^s$ over $\mathbb{F}_q$, where p is the characteristic of $\mathbb{F}_q$, ℓ is an odd prime different from p, and k is a prime different from ℓ and p. Batoul et al. [2] investigated the structure of constacyclic codes of length $2^a mp^r$ over $\mathbb{F}_{p^s}$ with $a \geq 1$ and $(m, p) = 1$. They also provided certain sufficient conditions under which these codes are equivalent to cyclic codes of length $2^a mp^r$ over $\mathbb{F}_{p^s}$. Sharma [16] determined all constacyclic codes of length $\ell^t p^s$ over $\mathbb{F}_{p^r}$ and their dual codes, where ℓ, p are distinct primes, ℓ is odd and s, t, r are positive integers. In 2016, Sharma et al. [17] determine generator polynomials of all constacyclic codes of length $4\ell^m p^n$ over the finite field $\mathbb{F}_q$ and their dual codes, where p, ℓ are distinct odd primes, q is a power of p and m, n are positive integers. Working in the same direction, Liu et al. obtained generator polynomials of all repeated-root constacyclic codes of length $3\ell p^s$ over $\mathbb{F}_q$ in [14], where ℓ is an odd prime different from p and 3. In 2017, Liu et al. [15] explicitly determine the generator polynomials of all repeated-root constacyclic codes of length $n\ell p^s$ over $\mathbb{F}_q$ and their dual codes, where ℓ is an odd prime different from p, and n is an odd prime different from both ℓ and p such that $n = 2h + 1$ for some prime h. In 2019, Wu and Yue et al. [19,20] explicitly factorize the polynomial $x^n - \lambda$ for each $\lambda \in \mathbb{F}_q$. As applications, they obtain all repeated-root λ-constacyclic codes and their dual codes of length np^s over $\mathbb{F}_q$.

In this paper, we answer the question of B. Chen, H. Dinh and Liu. That is we determine all the constacyclic codes of length $p_1 p_2^t p^s$ over $\mathbb{F}_q$, where p is the characteristic of $\mathbb{F}_q$, p_1 is an odd prime different from p, and p_1 is a prime different from p_2 and p. We give the explicit generator polynomials of all the constacyclic codes of length $p_1 p_2^t p^s$ over $\mathbb{F}_q$ and their dual codes, and determine all self-dual cyclic codes of length $p_1 p_2^t p^s$ and their enumeration.

The remainder of this paper is organized as follows. In Section 2 we give a brief background on some basic results which we need in the following parts. In Section 3, we calculate the q-cyclotomic cosets modulo $p_1 p_2^t$ as a preparation for giving the generator polynomials of constacyclic codes of length $p_1 p_2^t p^s$ over $\mathbb{F}_q$. In Section 4, we first describe a general method to obtain the generator polynomials of constacyclic codes, and then with this method and the results of q-cyclotomic cosets modulo $p_1 p_2^t$ we give the explicit generator polynomials of all the constacyclic codes of length $p_1 p_2^t p^s$. And in Section 5, all the self-dual cyclic codes of length $p_1 p_2^t p^s$ over $\mathbb{F}_q$ are given. In the last section, as an example we calculate the case of length $5\ell p^s$, where ℓ is a prime different from 5 and p.

2. Preliminaries

In this section, we first review some basic results in number theory and finite fields, which we will in the following parts, and then give a brief introduction to the λ-constacyclic codes. For a positive integer n, we denote by $\mathbb{Z}_n$ the ring of integers module n throughout this paper. Let p be a prime number, and q be a power of p. We denote by $\mathbb{F}_q$ the finite field with q elements, and fix a generator element ξ of the multiplicative group $\mathbb{F}_q^*$, that is, $\mathbb{F}_q^* = \langle\xi\rangle$. In this paper, we mainly deal with the repeated-root constacyclic codes of length $p_1p_2^tp^s$ over $\mathbb{F}_q$, where p_1 and p_2 are two distinct odd prime numbers different from p. For any positive integer d and $i = 1, 2$, we write $f_{i,d} = \mathrm{ord}_{p_i^d}(q)$ for the multiplicative order of q modulo p_i^d, and set $g_{i,d} = \dfrac{\phi(p_i^d)}{f_{i,d}}$, where ϕ is the Euler's phi function. When $d = 1$, we write $f_i = f_{i,1}$ and $g_i = g_{i,1}$ for simplicity. For $i = 1, 2$, there are positive integers u_i and w_i such that $q^{f_i} = 1 + p_i^{u_i}w_i$ and $p_i \nmid w_i$. Following the lifting-the-exponent lemma, we immediately have

$$f_{i,d} = f_ip_i^{max\{0,d-u_i\}}.$$

Lemma 2.1. *[12] Assume that r is a primitive root of the odd prime p and* $(r+tp)^{p-1}$ *is not congruent to* 1 *modulo* p^2*. Then* $r + tp$ *is a primitive root of* p^k *for each* $k \geq 1$.

Lemma 2.2. *[18] Let* $n \geq 2$ *be an integer, and* λ *be a nonzero element in* $\mathbb{F}_q$ *with multiplicative order* $k = \mathrm{ord}(\lambda)$*. The binomial* $x^n - \lambda$ *is irreducible over* $\mathbb{F}_q$ *if and only if*

(1) Every prime divisor of n divides k, but not $\frac{q-1}{k}$*;*

(2) If $4 \mid n$*, then* $4 \mid (q-1)$.

Let λ be a nonzero element in $\mathbb{F}_q$. A λ-constacyclic code of length n is a linear code C such that $(c_0, c_1, \cdots, c_{n-1}) \in C$ implies $(\lambda c_{n-1}, c_0, \cdots, c_{n-2}) \in C$. This definition is a natural generalization of cyclic code and negacyclic code. A λ-constacyclic code C of length n over $\mathbb{F}_q$ can be regarded as an ideal $(g(x))$ of the quotient ring $\mathbb{F}_q[x]/(x^n - \lambda)$, where $g(x)$ is a divisor of $x^n - \lambda$. Let C be a λ-constacyclic code of length n over $\mathbb{F}_q$, then the dual code of code C is given by $C^\perp = \{x \in \mathbb{F}_q^n : x \cdot y = 0, \forall y \in C\}$, where $x \cdot y$ denotes the Euclidean inner product of x and y. If C is generated by a polynomial $g(x)$ satisfying $g(x) \mid x^n - \lambda$, and $h(x)$ is given by $h(x) = \frac{x^n-\lambda}{g(x)}$, then $h(x)$ is called the parity check polynomial of code C. It is a classical result that the dual code $C^\perp$ is generated by $h(x)^*$, where $h(x)^* = h(0)^{-1}x^{deg(h(x))}h(x^{-1})$ is the reciprocal polynomial of $h(x)$. The code C is called to be a self-orthogonal if $C \subseteq C^\perp$ and a self-dual code if $C = C^\perp$. For self-dual cyclic code, a well-known result states that there exist self-dual cyclic codes of length n over $\mathbb{F}_q$ if and only if n is even and the characteristic of $\mathbb{F}_q$ is $p = 2$.

There are $q - 1$ classes of constacyclic codes of length n over $\mathbb{F}_q$. However, some of them are turned out to be equivalent in the sense that they have the same structure. To be explicit, two elements $\lambda, \mu \in \mathbb{F}_q^*$ are called n-equivalent in $\mathbb{F}_q^*$if there exists $a \in \mathbb{F}_q^*$ such that $a^n\lambda = \mu$.

Lemma 2.3. *[5] For any* $\lambda, \mu \in \mathbb{F}_q^*$*, the following four statements are equivalent:*

(1) λ *and* μ *are n-equivalent in* $\mathbb{F}_q^*$.

(2) $\lambda^{-1}\mu \in \langle\xi^n\rangle$.

(3) $(\lambda^{-1}\mu)^d = 1$*, where* $d = \frac{q-1}{gcd(n,q-1)}$.

(4) There exists an $a \in \mathbb{F}_q^*$ such that

$$\varphi_a : \mathbb{F}_q[X]/(X^n - \mu) \to \mathbb{F}_q[X]/(X^n - \lambda); f(X) \mapsto f(aX)$$

is an $\mathbb{F}_q$-algebra isomorphism. In particular, there are $\gcd(n, q-1)$ *n-equivalence classes in $\mathbb{F}_q^*$.*

We conclude this section with the introduction of q-cyclotomic coset which is important in the computation of constacyclic codes. Let n be a positive integer relatively prime to n. For $0 \leq s \leq n-1$, the q-cyclotomic coset of s modulo n is defined to be

$$C_s = \{s, sq, \cdots, sq^{n_s - 1}\},$$

where n_s is the least positive integer such that $sq^{n_s} \equiv s \pmod{n}$. It is obvious to see that n_s is equal to the multiplicative order of q modulo $\frac{n}{\gcd(s,n)}$. Notice that if $sq^a \equiv s'q^b \pmod{n}$ for some positive integers a, b, then

$$s \equiv sq^{a+(n_s-a)} \equiv s'q^{b+(n_s-a)} \pmod{n}.$$

It follows that for $0 \leq s, s' \leq n-1$, $C_s \cap C_{s'} \neq \emptyset$ if and only if $C_s = C_{s'}$. Therefore the q-cyclotomic cosets give a classification of the element in $\mathbb{Z}_n$.

If α is a primitive nth root of unit in some extension field of $\mathbb{F}_q$, then the polynomial

$$C_s(x) = \prod_{i \in C_s} (x - \alpha^i)$$

is exactly the minimal polynomial of α^s over $\mathbb{F}_q$, and

$$x^n - 1 = \prod_s C_s(x)$$

gives the irreducible factorization of $x^n - 1$ over $\mathbb{F}_q$, where s runs over all representations of distinct q-cyclotomic cosets modulo n. We call $C_s(x)$ the polynomial associated to C_s.

Let $C_s = \{s, sq, \cdots, sq^{n_s-1}\}$ be any q-cyclotomic coset modulo n. The reciprocal coset of C_s is defined to be

$$C_s^* = \{-s, -sq, \cdots, -sq^{n_s-1}\}.$$

We say that the coset C_s is self-reciprocal if $C_s = C_s^*$. One can check that the polynomial $C_s^*(x)$ associated to the reciprocal coset C_s^* is exactly the reciprocal polynomial of $C_s(x)$.

3. q-cyclotomic cosets modulo $p_1^{t_1} p_2^{t_2}$

The q-cyclotomic cosets modulo $p_1 p_2^t$ plays an important role in determining all the constacyclic codes of length $p_1 p_2^t p^s$. In this section we consider a more general case that classifies all the q-cyclotomic cosets modulo $p_1^{t_1} p_2^{t_2}$, where p_1 and p_2 are two distinct odd prime numbers not dividing q, and t_1, t_2 are positive integers.

Let ℓ be a prime number not dividing q, and μ be a generator of the cyclic group $\mathbb{Z}_\ell^*$. It is obvious that all the q-cyclotomic cosets modulo ℓ are given by $C_0 = \{0\}$ and

$$C_k = \{\mu^k, \mu^k q, \cdots, \mu^k q^{\mathrm{ord}_\ell(q)-1}\},\ 1 \leq k \leq \frac{\ell - 1}{\mathrm{ord}_\ell(q)}.$$

For different odd prime numbers p_1 and p_2, we claim that there exists an integer μ_1 satisfying that:
(1) μ_1 is a primitive root modulo p_1^d for all $d \geq 1$; and
(2) $\mu_1 \equiv 1 \pmod{p_2}$.
We begin with a random primitive root $\eta_1^{'}$ modulo p_1. If $p_1^2 \nmid \eta_1^{'\,p_1-1} - 1$, we let $\eta_1 = \eta_1^{'}$, otherwise we let $\eta_1 = \eta_1^{'} + p_1$. It is trivial to see that η_1 satisfies the condition $\gcd(\frac{\eta_1^{p_1-1}-1}{p_1}, p_1) = 1$. Let $\mu_1 = \eta_1 + (1-\eta_1)p_1^{p_2-1}$, then

$$\mu_1^{p_1-1} - 1 \equiv (\eta_1 + (1-\eta_1)p_1^{p_2-1})^{p_1-1} - 1 \equiv \eta_1^{p_1-1} - 1 \pmod{p_1^2}.$$

It follows that

$$\gcd(\frac{\mu_1^{p_1-1}-1}{p_1}, p_1) = \gcd(\frac{\eta_1^{p_1-1}-1}{p_1}, p_1) = 1.$$

Following Lemma 2.1, μ_1 is a primitive root modulo p_1^d for all $d \geq 1$ such that $\mu_1 \equiv 1 \pmod{p_2}$. By the symmetric argument, we can find an integer μ_2 satisfying that
(1) μ_2 is a primitive root modulo p_2^d for all $d \geq 1$; and
(2) $\mu_2 \equiv 1 \pmod{p_1}$.
We fix such a pair of integers μ_1 and μ_2.

Theorem 3.1. *Let p_1 and p_2 be two different odd prime numbers not dividing q, and t_1 and t_2 be positive integers. Then all the distinct q-cyclotomic cosets module $p_1^{t_1}p_2^{t_2}$ are given by*

$$C_{\mu_1^{k_1}\mu_2^{k_2}p_1^{r_1}p_2^{r_2}} = \{\mu_1^{k_1}\mu_2^{k_2}p_1^{r_1}p_2^{r_2}, \mu_1^{k_1}\mu_2^{k_2}p_1^{r_1}p_2^{r_2}q, \cdots, \mu_1^{k_1}\mu_2^{k_2}p_1^{r_1}p_2^{r_2}q^{c_{r_1,r_2}}\}$$

for $0 \leq r_1 \leq t_1$, $0 \leq r_2 \leq t_2$, $0 \leq k_1 \leq g_{1,t_1-r_1} - 1$ *and* $0 \leq k_2 \leq g_{2,t_2-r_2} \cdot \gcd(f_{1,t_1-r_1}, f_{2,t_2-r_2}) - 1$, *where* $c_{r_1,r_2} = \mathrm{ord}_{p_1^{t_1-r_1}p_2^{t_2-r_2}}(q) = \mathrm{lcm}(f_{1,t_1-r_1}, f_{2,t_2-r_2})$.

Proof. First we prove that the given q-cyclotomic cosets are all distinct. If $C_{\mu_1^{k_1}\mu_2^{k_2}p_1^{r_1}p_2^{r_2}} = C_{\mu_1^{k_1'}\mu_2^{k_2'}p_1^{r_1'}p_2^{r_2'}}$ for some $0 \leq r_1, r_1' \leq t_1, 0 \leq r_2, r_2' \leq t_2, 0 \leq k_1, k_1' \leq g_{1,t_1-r_1} - 1$ and $0 \leq k_2, k_2' \leq g_{2,t_2-r_2} \cdot \gcd(f_{1,t_1-r_1}, f_{2,t_2-r_2}) - 1$, then there exists a positive integer m such that

$$\mu_1^{k_1'}\mu_2^{k_2'}p_1^{r_1'}p_2^{r_2'} \equiv \mu_1^{k_1}\mu_2^{k_2}p_1^{r_1}p_2^{r_2}q^m \pmod{p_1^{t_1}p_2^{t_2}}. \tag{3.1}$$

Since μ_1, μ_2 and q are relatively prime to $p_1^{t_1}p_2^{t_2}$, clearly we have $r_1 = r_1'$ and $r_2 = r_2'$, and Eq (3.1) can be reduced to

$$\mu_1^{k_1'}\mu_2^{k_2'} \equiv \mu_1^{k_1}\mu_2^{k_2}q^m \pmod{p_1^{t_1-r_1}p_2^{t_2-r_2}}.$$

Remembering that $\mu_1 \equiv 1 \pmod{p_2}$ and $\mu_2 \equiv 1 \pmod{p_1}$, then by the Chinese remainder theorem, we have

$$\mu_1^{k_1-k_1'} \equiv q^m \pmod{p_1^{t_1-r_1}} \tag{3.2}$$

$$\mu_2^{k_2-k_2'} \equiv q^m \pmod{p_2^{t_2-r_2}} \tag{3.3}$$

Equation (3.2) implies that

$$\mu_1^{(k_1-k_1')f_{1,t_1-r_1}} \equiv q^{m \cdot f_{1,t_1-r_1}} \equiv 1 \pmod{p_1^{t_1-r_1}},$$

and therefore $\phi(p_1^{t_1-r_1}) \mid (k_1 - k_1')f_{1,t_1-r_1}$. Since $0 \le k_1, k_1' \le g_{1,t_1-r_1} - 1$, one must have $k_1 = k_1'$. Notice that $k_1 = k_1'$ indicates that $q^m \equiv 1 \pmod{p_1^{t_1-r_1}}$, then $f_{1,t_1-r_1} \mid m$, which together with Eq (3.3) leads to

$$\mu_2^{(k_2'-k_2)\cdot\frac{f_{2,t_2-r_2}}{\gcd(f_{1,t_1-r_1},f_{2,t_2-r_2})}} \equiv q^{m\cdot\frac{f_{2,t_2-r_2}}{\gcd(f_{1,t_1-r_1},f_{2,t_2-r_2})}} \equiv 1 \pmod{p_2^{t_2-r_2}}.$$

Thus $\phi(p_2^{t_2-r_2}) \mid (k_2' - k_2) \cdot \frac{f_{2,t_2-r_2}}{\gcd(f_{1,t_1-r_1},f_{2,t_2-r_2})}$. Since $0 \le k_2, k_2' \le g_{2,t_2-r_2} \cdot \gcd(f_{1,t_1-r_1}, f_{2,t_2-r_2}) - 1$, we have $k_2 = k_2'$.

On the other hand, there are in total

$$\begin{aligned}&\sum_{0\le r_1\le t_1}\sum_{0\le r_2\le t_2} \frac{\phi(p_1^{t_1-r_1})}{f_{1,t_1-r_1}} \cdot \frac{\phi(p_2^{t_2-r_2})}{f_{2,t_2-r_2}} \cdot \gcd(f_{1,t_1-r_1}, f_{2,t_2-r_2}) \cdot \mathrm{lcm}(f_{1,t_1-r_1}, f_{2,t_2-r_2})\\ =& \sum_{0\le r_1\le t_1}\sum_{0\le r_2\le t_2} \phi(p_1^{t_1-r_1})\phi(p_2^{t_2-r_2}) = p_1^{t_1}p_2^{t_2}\end{aligned} \tag{3.4}$$

elements in these q-cyclotomic cosets, therefore they are all the distinct q-cyclotomic cosets module $p_1^{t_1}p_2^{t_2}$. □

In particular, when $t_1 = 1$ and $t_2 = t$, the classification of the q-cyclotomic cosets modulo $p_1p_2^t$ is given as follow.

Corollary 3.1. *Let the notations be as above. Then all the distinct q-cyclotomic cosets modulo $p_1p_2^t$ are*

$$C_0 = \{0\};$$

$$C_{\mu_1^{k_1}\mu_2^{k_2}p_2^r} = \{\mu_1^{k_1}\mu_2^{k_2}p_2^r, \mu_1^{k_1}\mu_2^{k_2}p_2^r q, \cdots, \mu_1^{k_1}\mu_2^{k_2}p_2^r q^{\mathrm{ord}_{p_1p_2^{t-r}}(q)-1}\}$$

for $0 \le r \le t-1$, $0 \le k_1 \le g_1 - 1$ *and* $0 \le k_2 \le g_{2,t-r} \cdot \gcd(f_1, f_{2,t-r})$*;*

$$C_{\mu_1^k p_2^t} = \{\mu_1^k p_2^t, \mu_1^k p_2^t q, \cdots, \mu_1^k p_2^t q^{f_1-1}\}$$

for $0 \le k \le g_1 - 1$*; and*

$$C_{\mu_2^{k'} p_1p_2^r} = \{\mu_2^{k'} p_1p_2^r, \mu_2^{k'} p_1p_2^r q, \cdots, \mu_2^{k'} p_1p_2^r q^{f_{2,t-r}-1}\}$$

for $0 \le r \le t-1$ *and* $0 \le k' \le g_{2,t-r} - 1$.

Corollary 3.2. *Let the notations be as aboved. Then the irreducible factorization of $x^{p_1p_2^tp^s} - 1$ over $\mathbb{F}_q$ is given by*

$$x^{p_1p_2^tp^s} - 1 = C_0(x)^{p^s} \prod_{r=0}^{t-1}\prod_{k_1=0}^{g_1-1}\prod_{k_2=0}^{g_{2,t-r}\gcd(f_1,f_{2,t-r})-1} C_{\mu_1^{k_1}\mu_2^{k_2}p_2^r}(x)^{p^s} \prod_{k=0}^{g_1-1} C_{\mu_1^k p_2^t}(x)^{p^s} \prod_{r=0}^{t-1}\prod_{k'=0}^{g_{2,t-r}-1} C_{\mu_2^{k'}p_1p_2^r}(x)^{p^s}.$$

4. Constacyclic codes of length $p_1p_2^tp^s$ with their dual codes

In this section, we will determine the generator polynomials of all constacyclic codes of length $p_1p_2^tp^s$ over $\mathbb{F}_q$ and their dual codes. For $\lambda \in \mathbb{F}_q^*$, we identify a λ-constacyclic code of length $p_1p_2^tp^s$ with an ideal $(g(x))$ of the quotient ring $\mathbb{F}_q[x]/(x^{p_1p_2^tp^s} - \lambda)$, where $g(x)$ is a divisor of $x^{p_1p_2^tp^s} - \lambda$. By Lemma 2.3, there are $\gcd(p_1p_2^t, q-1)$ $p_1p_2^tp^s$-equivalence classes in $\mathbb{F}_q^*$, which corresponds to the cosets of $\langle \xi^{p_1p_2^t} \rangle$ in $\mathbb{F}_q^* = \langle \xi \rangle$.

Before doing the explicit computation, we present a general method to factorize $x^n - \lambda$. Let $q = p^k$ for $k > 0$, and $n = p^e p_1^{e_1} \cdots p_m^{e_m}$ be the prime factorization of n. Assume that $p_1^{e_1} \cdots p_m^{e_m} \mid q-1$, i.e., $v_{p_i}(q-1) \geq e_i$ for $i = 1, \cdots, m$. In this case we have

$$\mathbb{F}_q^* = \langle \xi \rangle = \langle \xi^{p_1^{e_1}\cdots p_m^{em}} \rangle \cup \langle \xi^{p_1^{e_1}\cdots p_m^{em}} \rangle \xi^{p^e} \cup \cdots \cup \langle \xi^{p_1^{e_1}\cdots p_m^{em}} \rangle \xi^{p^e(p_1^{e_1}\cdots p_m^{em}-1)}.$$

For $\lambda \in \langle \xi^{p_1^{e_1}\cdots p_m^{em}} \rangle \xi^{j\cdot p^e}$, where $0 \leq j \leq p_1^{e_1} \cdots p_m^{e_m} - 1$, there exists an element $a \in \mathbb{F}_q^*$ such that

$$a^n \lambda = \xi^{j\cdot p^e}.$$

We first factorize $x^n - \xi^{jp^e}$, $0 \leq j \leq p_1^{e_1} \cdots p_m^{e_m} - 1$. Notice that j can be written as $j = y \cdot p_1^{v_1} \cdots p_m^{v_m}$, where $v_i = min\{e_i, v_{p_i}(j)\}$. Then we have

$$x^n - \xi^{j\cdot p^e} = (x^{p_1^{e_1}\cdots p_m^{em}} - \xi^{y\cdot p_1^{v_1}\cdots p_m^{vm}})^{p^e} = \xi^{j\cdot p^e}((\frac{x^{p_1^{e_1-v_1}\cdots p_m^{em-vm}}}{\xi^y})^{p_1^{v_1}\cdots p_m^{vm}} - 1)^{p^e}.$$

Since $p_1^{v_1} \cdots p_m^{v_m} \mid q-1$, $\delta = \xi^{\frac{q-1}{p_1^{v_1}\cdots p_m^{vm}}}$ is a primitive $p_1^{v_1} \cdots p_m^{v_m}$-th root of unit. Then

$$\begin{aligned} x^n - \xi^{j\cdot p^e} &= \xi^{j\cdot p^e}(\frac{x^{p_1^{e_1-v_1}\cdots p_m^{em-vm}}}{\xi^y} - 1)^{p^e} \cdot (\frac{x^{p_1^{e_1-v_1}\cdots p_m^{em-vm}}}{\xi^y} - \delta)^{p^e} \cdots (\frac{x^{p_1^{e_1-v_1}\cdots p_m^{em-vm}}}{\xi^y} - \delta^{p_1^{v_1}\cdots p_m^{vm}-1})^{p^e} \\ &= (x^{p_1^{e_1-v_1}\cdots p_m^{em-vm}} - \xi^y)^{p^e}(x^{p_1^{e_1-v_1}\cdots p_m^{em-vm}} - \delta\xi^y)^{p^e} \cdots (x^{p_1^{e_1-v_1}\cdots p_m^{em-vm}} - \delta^{p_1^{v_1}\cdots p_m^{vm}-1}\xi^y)^{p^e}. \end{aligned}$$

For $0 \leq i \leq p_1^{v_1} \cdots p_m^{v_m} - 1$, $\delta^i\xi^y = \xi^{y+i\cdot\frac{q-1}{p_1^{v_1}\cdots p_m^{vm}}}$, and then we have

$$\mathrm{ord}(\delta^i\xi^y) = \frac{q-1}{gcd(q-1, y+i\cdot\frac{q-1}{p_1^{v_1}\cdots p_m^{vm}})},$$

and

$$\frac{q-1}{\mathrm{ord}(\delta^i\xi^y)} = \gcd(q-1, y+i\cdot\frac{q-1}{p_1^{v_1}\cdots p_m^{v_m}}).$$

For each $p_i \mid p_1^{e_1-v_1} \cdots p_m^{e_m-v_m}$, we have that $e_i > v_i$ and $v_i = v_{p_i}(j)$, thus $p_i \nmid y$. Since $v_{p_i}(q-1) \geq e_i > v_i$, $p_i \mid \frac{q-1}{p_1^{v_1}\cdots p_m^{vm}}$, which indicates that $p_i \nmid y + i\cdot\frac{q-1}{p_1^{v_1}\cdots p_m^{vm}}$ and $p_i \mid \frac{q-1}{y+i\cdot\frac{q-1}{p_1^{v_1}\cdots p_m^{vm}}}$. Moreover if $4 \mid p_1^{e_1-v_1} \cdots p_m^{e_m-v_m}$, then $4 \mid p_1^{e_1} \cdots p_m^{e_m} \mid q-1$. Hence by Lemma 2.2 each $x^{p_1^{e_1-v_1}\cdots p_m^{em-vm}} - \xi^y\delta^i$ is irreducible over $\mathbb{F}_q$.

Notice that $a^n\lambda = \xi^{jp^e}$, then the irreducible factorization of $x^n - \lambda$ follows immediately:

$$\begin{aligned} x^n - \lambda &= (x^{p_1^{e_1-v_1}\cdots p_m^{em-vm}} - a^{-p_1^{e_1-v_1}\cdots p_m^{em-vm}}\xi^y)^{p^e}(x^{p_1^{e_1-v_1}\cdots p_m^{em-vm}} - a^{-p_1^{e_1-v_1}\cdots p_m^{em-vm}}\delta\xi^y)^{p^e} \cdot \\ &\quad \cdots \cdot (x^{p_1^{e_1-v_1}\cdots p_m^{em-vm}} - a^{-p_1^{e_1-v_1}\cdots p_m^{em-vm}}\delta^{p_1^{v_1}\cdots p_m^{vm}-1}\xi^y)^{p^e}, \end{aligned}$$

We summerize the above discussions into the following theorem.

Theorem 4.1. *Let $p, p_1, \cdots, p_m$ be distinct prime numbers. Let $q = p^k$ and $n = p^e p_1^{e_1} \cdots p_m^{e_m}$, where $k, e, e_1, \cdots, e_m$ are positive integers. Suppose that for $1 \leq i \leq m$, $v_{p_i}(q-1) \geq e_i$. Then for any $\lambda \in \mathbb{F}_q^*$, there exists an element $a \in \mathbb{F}_q^*$ such that $a^n \lambda = \xi^{jp^e}$, $0 \leq j \leq p_1^{e_1} \cdots p_m^{e_m}$. Furthermore, writing j in the form $j = y \cdot p_1^{v_1} \cdots p_m^{v_m}$, where $v_i = min\{e_i, v_{p_i}(j)\}$, then*

$$\begin{aligned} x^n - \lambda &= (x^{p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} - a^{-p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} \xi^y)^{p^e} (x^{p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} - a^{-p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} \delta \xi^y)^{p^e} \cdot \\ &\quad \cdots \cdot (x^{p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} - a^{-p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} \delta^{p_1^{v_1}\cdots p_m^{v_m}-1} \xi^y)^{p^e}, \end{aligned}$$

gives the irreducible factorization of $x^n - \lambda$ over $\mathbb{F}_q$.

Now we turn to the case that $p_1^{e_1} \cdots p_m^{e_m} \nmid q-1$. Sinve $\gcd(p_1^{e_1} \cdots p_m^{e_m}, q) = 1$, thus there exists a least positive integer d such that $p_1^{e_1} \cdots p_m^{e_m} \mid q^d - 1$. By the lifting-the-exponent lemma, if d' is the least positive integer such that $p_1 \cdots p_m \mid q^{d'} - 1$, then $d = d' p_1^{v_1} \cdots p_m^{v_m}$, where $v_i = \max\{e_i - v_{p_i}(q^{d'} - 1), 0\}$.

Let λ be a nonzero element in $\mathbb{F}_q$. To obtain the irreducible factorization of $x^n - \lambda$ over $\mathbb{F}_q$, we first consider the factorization over $\mathbb{F}_{q^d}$. By Theorem 4.1, there exists $a \in \mathbb{F}_{q^d}$ such that $a^n \lambda = \zeta^{jp^e}$, $0 \leq j \leq p_1^{e_1} \cdots p_m^{e_m} - 1$. Writing j as $j = y \cdot p_1^{v_1} \cdots p_m^{v_m}$, where $v_i = min\{e_i, v_{p_i}(j)\}$, then

$$\begin{aligned} x^n - \lambda &= (x^{p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} - a^{-p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} \zeta^y)^{p^e} (x^{p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} - a^{-p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} \delta \zeta^y)^{p^e} \cdot \\ &\quad \cdots \cdot (x^{p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} - a^{-p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} \delta^{p_1^{v_1}\cdots p_m^{v_m}-1} \zeta^y)^{p^e}, \end{aligned}$$

gives the irreducible factorization of $x^n - \lambda$ over $\mathbb{F}_{q^d}$, where δ is a primitive $p_1^{v_1} \cdots p_m^{v_m}$-th root of unit. Hence each irreducible factor of $x^n - \lambda$ over $\mathbb{F}_q$ is of the form

$$\begin{aligned} &(x^{p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} - a^{-p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} \delta^i \zeta^y)^{p^e} (x^{p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} - a^{-qp_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} \delta^{qi} \zeta^{qy})^{p^e} \cdot \\ &\cdots \cdot (x^{p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} - a^{-q^{z_i-1} p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} \delta^{i \cdot q^{z_i-1}} \zeta^{y \cdot q^{z_i-1}})^{p^e}, \end{aligned}$$

where z_i is the least positive integer such that $a^{-q^{z_i} p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} \delta^{i \cdot q^{z_i}} \zeta^{y \cdot q^{z_i}} = a^{-p_1^{e_1-v_1}\cdots p_m^{e_m-v_m}} \delta^i \zeta^y$.

Now we determine the generator polynomials of all constacyclic codes of length $p_1 p_2^t p^s$ and their duals explicitly. We decompose the problem into three cases.

4.1. $\gcd(q-1, p_1 p_2^t p^s) = 1$

As $\gcd(q-1, p_1 p_2^t p^s) = 1$, all constacyclic codes of length $p_1 p_2^t p^s$ are equivalent to a cyclic code. By the factorization of $x^{p_1 p_2^t p^s} - 1$ given in Corollary 3.2, we have the following result. For any polynomial

$$F = a_0 + a_1 x + \cdots + a_n x^n, \ a_n \neq 0,$$

we set $\widehat{F} = a_n^{-1} F$ to be the monic polynomial associated to F.

Proposition 4.1. *Assume that* $\gcd(q-1, p_1 p_2^t p^s) = 1$. *Then any nonzero element λ in $\mathbb{F}_q$ is $p_1 p_2^t p^s$-equivalent to 1, that is, there is an element $a \in \mathbb{F}_q^*$ such that $a^{p_1 p_2^t p^s} \lambda = 1$. Furthermore, the irreducible factorization of $x^{p_1 p_2^t p^s} - \lambda$ over $\mathbb{F}_q$ is given by*

$$x^{p_1 p_2^t p^s} - \lambda = \widehat{C}_0(ax)^{p^s} \prod_{r=0}^{t-1} \prod_{k_1=0}^{g_1-1} \prod_{k_2=0}^{g_{2,t-r} \gcd(f_1, f_{2,t-r})-1} \widehat{C}_{\mu_1^{k_1} \mu_2^{k_2} p_2^r}(ax)^{p^s} \prod_{k=0}^{g_1-1} \widehat{C}_{\mu_1^k p_2^t}(ax)^{p^s} \prod_{r=0}^{t-1} \prod_{k'=0}^{g_{2,t-r}-1} \widehat{C}_{\mu_2^{k'} p_1 p_2^r}(ax)^{p^s}.$$

Therefore all the constacyclic codes of length $p_1p_2^tp^s$ *are*

$$C=\left(\widehat{C}_0(ax)^u\prod_{r=0}^{t-1}\prod_{k_1=0}^{g_1-1}\prod_{k_2=0}^{g_{2,t-r}\gcd(f_1,f_{2,t-r})-1}\widehat{C}_{\mu_1^{k_1}\mu_2^{k_2}p_2^r}(ax)^{v_{\mu_1^{k_1}\mu_2^{k_2}p_2^r}}\prod_{k=0}^{g_1-1}\widehat{C}_{\mu_1^kp_2^t}(ax)^{w_{\mu_1^kp_2^t}}\prod_{r=0}^{t-1}\prod_{k'=0}^{g_{2,t-r}-1}\widehat{C}_{\mu_2^{k'}p_1p_2^r}(ax)^{x_{\mu_2^{k'}p_1p_2^r}}\right),$$

where $0\le u,v_{\mu_1^{k_1}\mu_2^{k_2}p_2^r},w_{\mu_1^kp_2^t},x_{\mu_2^{k'}p_1p_2^r}\le p^s$, *with duals*

$$\begin{aligned}C^\perp\ =\ &\left(\widehat{C}_0(a^{-1}x)^{p^s-u}\prod_{r=0}^{t-1}\prod_{k_1=0}^{g_1-1}\prod_{k_2=0}^{g_{2,t-r}\gcd(f_1,f_{2,t-r})-1}\widehat{C}_{\mu_1^{k_1}\mu_2^{k_2}p_2^r}(a^{-1}x)^{p^s-v_{\mu_1^{k_1}\mu_2^{k_2}p_2^r}}\prod_{k=0}^{g_1-1}\widehat{C}_{\mu_1^kp_2^t}(a^{-1}x)^{p^s-w_{\mu_1^kp_2^t}}\right.\\&\left.\prod_{r=0}^{t-1}\prod_{k'=0}^{g_{2,t-r}-1}\widehat{C}_{\mu_2^{k'}p_1p_2^r}(a^{-1}x)^{p^s-x_{\mu_2^{k'}p_1p_2^r}}\right).\end{aligned}$$

4.2. $\gcd(q-1,p_1p_2^tp^s)=p_1p_2^t$

For this case, since $p_1p_2^t|q-1$, the following proposition follows straightly from Theorem 4.1.

Theorem 4.2. *Assume that* $\gcd(q-1,p_1p_2^tp^s)=p_1p_2^t$. *Then for any* $\lambda\in\mathbb{F}_q^*$, *there exists an element* $a\in\mathbb{F}_q^*$ *such that* $a^{p_1p_2^tp^s}\lambda=\xi^{j\cdot p^s}$, $0\le j\le p_1p_2^t-1$. *Writing* j *as* $j=y\cdot p_1^{v_1}p_2^{v_2}$, *where* $v_1=\min\{1,v_{p_1}(j)\}$ *and* $v_2=\min\{t,v_{p_2}(j)\}$, *then*

$$\begin{aligned}x^{p_1p_2^tp^s}-\lambda\ =\ &(x^{p_1^{1-v_1}p_2^{t-v_2}}-a^{-p_1^{1-v_1}p_2^{t-v_2}}\xi^y)^{p^s}(x^{p_1^{1-v_1}p_2^{t-v_2}}-a^{-p_1^{1-v_1}p_2^{t-v_2}}\delta\xi^y)^{p^s}\\&\cdots(x^{p_1^{1-v_1}p_2^{t-v_2}}-a^{-p_1^{1-v_1}p_2^{t-v_2}}\delta^{p_1^{v_1}p_2^{v_2}-1}\xi^y)^{p^s}\end{aligned}$$

gives the irreducible factorization of $x^{p_1p_2^tp^s}-\lambda$ *over* $\mathbb{F}_q$. *Therefore all the* λ*-constacyclic codes of length* $p_1p_2^tp^s$ *and their dual codes are given by*

$$\begin{aligned}C\ =\ &\left((x^{p_1^{1-v_1}p_2^{t-v_2}}-a^{-p_1^{1-v_1}p_2^{t-v_2}}\xi^y)^{u_1}(x^{p_1^{1-v_1}p_2^{t-v_2}}-a^{-p_1^{1-v_1}p_2^{t-v_2}}\delta\xi^y)^{u_2}\right.\\&\left.\cdots(x^{p_1^{1-v_1}p_2^{t-v_2}}-a^{-p_1^{1-v_1}p_2^{t-v_2}}\delta^{p_1^{v_1}p_2^{v_2}-1}\xi^y)^{u_{p_1^{v_1}p_2^{v_2}}}\right),\end{aligned}$$

and

$$\begin{aligned}C^\perp\ =\ &\left((x^{p_1^{1-v_1}p_2^{t-v_2}}-a^{p_1^{1-v_1}p_2^{t-v_2}}\xi^{-y})^{p^s-u_1}(x^{p_1^{1-v_1}p_2^{t-v_2}}-a^{p_1^{1-v_1}p_2^{t-v_2}}\delta^{-1}\xi^{-y})^{p^s-u_2}\right.\\&\left.\cdots(x^{p_1^{1-v_1}p_2^{t-v_2}}-a^{p_1^{1-v_1}p_2^{t-v_2}}\delta^{1-p_1^{v_1}p_2^{v_2}}\xi^{-y})^{p^s-u_{p_1^{v_1}p_2^{v_2}}}\right),\end{aligned}$$

where $0\le u_1,u_2,\cdots,u_{n^{v_1}\ell^{v_2}}\le p^s$.

4.3. $\gcd(q-1,p_1p_2^tp^s)=p_2^r$ *for some* $0<r\le t$

In this case, for any $d\ge1$ we have $f_{2,d}=p_2^{max\{0,d-r\}}$, and $f=\mathrm{lcm}(f_1,f_{2,t})$ is the least positive integer such that $q^f\equiv1\pmod{p_1p_2^t}$. By the bais results of finite fields, there is a primitive element ζ in $\mathbb{F}_{q^f}^*$ such that $\xi=\zeta^{\frac{q^f-1}{q-1}}=\zeta^{1+q+\cdots+q^{f-1}}$. Then we have

$$\mathbb{F}_q^*=\langle\xi\rangle=\langle\xi^{p_2^r}\rangle\cup\langle\xi^{p_2^r}\rangle\xi^{p^s}\cup\cdots\cup\langle\xi^{p_2^r}\rangle\xi^{(p_2^r-1)p^s}$$

and

$$\mathbb{F}_{q^f}^* = \langle \zeta \rangle = \langle \zeta^{p_1p_2^t} \rangle \cup \langle \zeta^{p_1p_2^t} \rangle \zeta^{p^s} \cup \cdots \cup \langle \zeta^{p_1p_2^t} \rangle \zeta^{(p_1p_2^t-1)p^s}.$$

By the assumption that $p_1p_2^t \mid q^f - 1$ and $v_{p_1}(q-1) = 0$, $v_{p_2}(q-1) = r$, we have that $p_1p_2^{t-r} \mid (1 + q + \cdots + q^{f-1})$. Therefore $\xi^{p_2^r} = \zeta^{p_2^r(1+q+\cdots+q^{f-1})} \in \langle \zeta^{p_1p_2^t} \rangle$. Furthermore, for $0 \le j \le p_2^r - 1$, there exists some $0 \le j' \le p_1p_2^t - 1$ such that $jp^s(1 + q + \cdots + q^{f-1}) \equiv j'p^s \pmod{p_1p_2^t}$, that is, $\xi^{jp^s} \in \langle \zeta^{p_1p_2^t} \rangle \zeta^{j'p^s}$. Hence we have the following theorem.

Theorem 4.3. *Assume that* $\gcd(q-1, p_1p_2^tp^s) = p_2^r$, $0 < r \le t$. *For any* $0 \le j \le p_2^r - 1$, *there exists an element* $a \in \mathbb{F}_{q^f}^*$ *such that* $a^{p_1p_2^tp^s}\xi^{j\cdot p^s} = \zeta^{j'\cdot p^s}$. *Moreover, each irreducible factor of* $x^{p_1p_2^t} - \xi^j$ *over* $\mathbb{F}_q$ *is of the form*

$$\begin{aligned}&(x^{p_1^{1-v_1}p_2^{t-v_2}} - a^{-p_1^{1-v_1}p_2^{t-v_2}}\delta^i\zeta^{y'})(x^{p_1^{1-v_1}p_2^{t-v_2}} - a^{-p_1^{1-v_1}p_2^{t-v_2}\cdot q}\delta^{iq}\zeta^{y'q})\\ &\cdots(x^{p_1^{1-v_1}p_2^{t-v_2}} - a^{-p_1^{1-v_1}p_2^{t-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y'q^{z_i-1}}),\end{aligned}$$

where $j' = y'p_1^{v_1}p_2^{v_2}$, $v_1 = \min\{1, v_{p_1}(j')\}$, $v_2 = \min\{t, v_{p_2}(j')\}$, *and* z_i *is the least positive integer such that* $a^{-q^{z_i}p_1^{1-v_1}p_2^{t-v_2}}\delta^{iq^{z_i}}\zeta^{y'q^{z_i}} = a^{p_1^{1-v_1}p_2^{t-v_2}}\delta^i\zeta^{y'}$.

For any $0 \le i, i' \le p_1^{v_1}p_2^{v_2} - 1$, we define a relation $\sim$ to be such that $i \sim i'$ if and only if $a^{-q^mp_1^{1-v_1}p_2^{t-v_2}}\delta^{iq^m}\zeta^{y'q^m} = a^{p_1^{1-v_1}p_2^{t-v_2}}\delta^{i'}\zeta^{y'}$ for some nonnegative integers m. It is obvious to see that $\sim$ is an equivalence relation. Assume that S is a complete system of equivalence class representatives of $\{0, 1, \cdots, p_1^{v_1}p_{\text{ffl}}^{v_2} - 1\}$ relative to this relation $\sim$. For any $i \in S$ we denote the irreducible polynomial

$$\begin{aligned}&(x^{p_1^{1-v_1}p_2^{t-v_2}} - a^{-p_1^{1-v_1}p_2^{t-v_2}}\delta^i\zeta^{y'})(x^{p_1^{1-v_1}p_2^{t-v_2}} - a^{-p_1^{1-v_1}p_2^{t-v_2}\cdot q}\delta^{iq}\zeta^{y'q})\\ &\cdots(x^{p_1^{1-v_1}p_2^{t-v_2}} - a^{-p_1^{1-v_1}p_2^{t-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y'q^{z_i-1}}),\end{aligned}$$

by $M_i(x)$. Then we have the following corollary.

Corollary 4.1. *Assume that* $\gcd(q-1, p_1p_2^tp^s) = p_2^r$. *For any* $0 \le j \le p_2^r - 1$, *there exists an element* $a \in \mathbb{F}_{q^f}^*$ *such that* $a^{p_1p_2^tp^s}\xi^{j\cdot p^s} = \zeta^{j'\cdot p^s}$. *Then*

$$x^{p_1p_2^tp^s} - \xi^{jp^s} = \prod_{i\in S} M_i(x)^{p^s}$$

gives the irreducible factorization of $x^{p_1p_2^tp^s} - \xi^{jp^s}$ *over* $\mathbb{F}_q$. *Furthermore we have that*

$$C = \left(\prod_{i\in S} M_i(x)^{u_i}\right),$$

and

$$C^{\perp} = \left(\prod_{i\in S} M_i^*(x)^{p^s-u_i}\right),$$

where $0 \le u_i \le p^s$, *for* $i \in S$.

4.4. $\gcd(q-1, p_1p_2^tp^s) = p_1p_2^r$ *for some* $0 < r < t$

The same argument as in the last section can be applied in this situation, only noticing that the least positive integer f such that $q^f \equiv 1 \pmod{p_1p_2^t}$ is $f = f_{2,t} = p_2^{\max\{0,t-r\}}$. We find a primitive element ζ in $\mathbb{F}_{q^f}^*$ such that $\xi = \zeta^{\frac{q^f-1}{q-1}} = \zeta^{1+q+\cdots+q^{f-1}}$, then

$$\mathbb{F}_q^* = \langle \xi \rangle = \langle \xi^{p_1p_2^r} \rangle \cup \langle \xi^{p_1p_2^r} \rangle \xi^{p^s} \cup \cdots \cup \langle \xi^{p_1p_2^r} \rangle \xi^{(p_2^r-1)p^s}$$

and

$$\mathbb{F}_{q^f}^* = \langle \zeta \rangle = \langle \zeta^{p_1p_2^t} \rangle \cup \langle \zeta^{p_1p_2^t} \rangle \zeta^{p^s} \cup \cdots \cup \langle \zeta^{p_1p_2^t} \rangle \zeta^{(p_1p_2^t-1)p^s}.$$

By the assumption that $p_1p_2^t \mid q^f - 1$ and $v_{p_2}(q-1) = r$, we have that $p_2^{t-r} \mid (1 + q + \cdots + q^{f-1})$, and $\xi^{p_1p_2^r} = \zeta^{p_1p_2^r(1+q+\cdots+q^{f-1})} \in \langle \zeta^{p_1p_2^t} \rangle$. Furthermore, for $0 \le j \le p_1p_2^r - 1$, there exists some $0 \le j' \le p_1p_2^t - 1$ such that $jp^s(1 + q + \cdots + q^{f-1}) \equiv j'p^s \pmod{p_1p_2^t}$, that is, $\xi^{jp^s} \in \langle \zeta^{p_1p_2^t} \rangle \zeta^{j'p^s}$. Hence we have the following theorem.

Theorem 4.4. *Assume that* $\gcd(q-1, p_1p_2^tp^s) = p_1p_2^r$ *for* $0 < r < t$, *then for any* $0 \le j \le p_2^r - 1$, *there exists an element* $a \in \mathbb{F}_{q^f}^*$ *such that* $a^{p_1p_2^tp^s}\xi^{j\cdot p^s} = \zeta^{j'\cdot p^s}$. *Moreover, each irreducible factor of* $x^{p_1p_2^t} - \xi^j$ *over* $\mathbb{F}_q$ *is of the form*

$$\begin{aligned}&(x^{p_1^{1-v_1}p_2^{t-v_2}} - a^{-p_1^{1-v_1}p_2^{t-v_2}}\delta^i\zeta^{y'})(x^{p_1^{1-v_1}p_2^{t-v_2}} - a^{-p_1^{1-v_1}p_2^{t-v_2}\cdot q}\delta^{iq}\zeta^{y'q})\\ &\cdots(x^{p_1^{1-v_1}p_2^{t-v_2}} - a^{-p_1^{1-v_1}p_2^{t-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y'q^{z_i-1}}),\end{aligned}$$

where $j' = y'p_1^{v_1}p_2^{v_2}$, $v_1 = \min\{1, v_{p_1}(j')\}$, $v_2 = \min\{t, v_{p_2}(j')\}$, *and* z_i *is the least positive integer such that* $a^{-q^{z_i}p_1^{1-v_1}p_2^{t-v_2}}\delta^{iq^{z_i}}\zeta^{y'q^{z_i}} = a^{p_1^{1-v_1}p_2^{t-v_2}}\delta^i\zeta^{y'}$.

For any $0 \le i, i' \le p_1^{v_1}p_2^{v_2} - 1$, we define a relation $\sim$ to be such that $i \sim i'$ if and only if $a^{-q^m p_1^{1-v_1}p_2^{t-v_2}}\delta^{iq^m}\zeta^{y'q^m} = a^{p_1^{1-v_1}p_2^{t-v_2}}\delta^{i'}\zeta^{y'}$ for some nonnegative integers m. It is obvious to see that $\sim$ is an equivalence relation. Assume that S is a complete system of equivalence class representatives of $\{0, 1, \cdots, p_1^{v_1}p_2^{v_2} - 1\}$ relative to this relation $\sim$. For any $i \in S$ we denote the irreducible polynomial

$$\begin{aligned}&(x^{p_1^{1-v_1}p_2^{t-v_2}} - a^{-p_1^{1-v_1}p_2^{t-v_2}}\delta^i\zeta^{y'})(x^{p_1^{1-v_1}p_2^{t-v_2}} - a^{-p_1^{1-v_1}p_2^{t-v_2}\cdot q}\delta^{iq}\zeta^{y'q})\\ &\cdots(x^{p_1^{1-v_1}p_2^{t-v_2}} - a^{-p_1^{1-v_1}p_2^{t-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y'q^{z_i-1}}),\end{aligned}$$

by $M_i(x)$. Then we have the following corollary.

Corollary 4.2. *Assume that* $\gcd(q-1, p_1p_2^tp^s) = p_1p_2^r$ *for* $0 < r < t$. *For any* $0 \le j \le p_2^r - 1$, *there exists an element* $a \in \mathbb{F}_{q^f}^*$ *such that* $a^{p_1p_2^tp^s}\xi^{j\cdot p^s} = \zeta^{j'\cdot p^s}$. *Then*

$$x^{p_1p_2^tp^s} - \xi^{jp^s} = \prod_{i \in Z} M_i(x)^{p^s}$$

gives the irreducible factorization of $x^{p_1p_2^tp^s} - \xi^{jp^s}$ *over* $\mathbb{F}_q$. *Furthermore we have that*

$$C = \left(\prod_{i \in S} M_i(x)^{u_i} \right),$$

and

$$C^{\perp} = \left(\prod_{i \in S} M_i^*(x)^{p^s - u_i} \right),$$

where $0 \leq u_i \leq p^s$, *for* $i \in S$.

5. All self-dual cyclic codes of length $p_1 p_2^t p^s$ over $\mathbb{F}_q$

Based on the results in the last section, we now give all the self-dual cyclic codes of length $p_1 p_2^t p^s$ over $\mathbb{F}_q$ and their enumeration. It is a well-known conclusion that self-dual cyclic codes of length N over $\mathbb{F}_q$ exists if and only if N is even and the characteristic of $\mathbb{F}_q$ is 2. Therefore we only consider the case of self-dual cyclic codes of length $p_1 p_2^t \cdot 2^s$ over $\mathbb{F}_{2^k}$.

Let $x^{p_1 p_2^t 2^s} - 1 = (x^{p_1 p_2^t} - 1)^{2^s} = f_1(x)^{2^s} \cdots f_n(x)^{2^s} h_1(x)^{2^s} \cdots h_m(x)^{2^s} h_1^*(x)^{2^s} \cdots h_m^*(x)^{2^s}$ be the irreducible factorization of $x^{p_1 p_2^t 2^s} - 1$ over $\mathbb{F}_q$, where each $f_i(x)$ is a monic irreducible self-reciprocal polynomial for $1 \leq i \leq n$, and $h_j^*(x)$ is the reciprocal polynomial of $h_j(x)$ for each $1 \leq j \leq m$. Now, given a cyclic code $C = (g(x))$ of length $p_1 p_2^t 2^s$, it can be written in the form

$$g(x) = f_1(x)^{\tau_1} \cdots f_n(x)^{\tau_n} h_1(x)^{\delta_1} \cdots h_m(x)^{\delta_m} h_1^*(x)^{\sigma_1} \cdots h_m^*(x)^{\sigma_m},$$

where $0 \leq \tau_i, \delta_j, \sigma_j \leq 2^s$ for any $1 \leq i \leq n$ and $1 \leq j \leq m$. Then the reciprocal polynomial $h^*(x)$ of the parity check polynomial $h(x)$ of C is

$$h^*(x) = f_1(x)^{2^s - \tau_1} \cdots f_n(x)^{2^s - \tau_n} h_1(x)^{2^s - \sigma_1} \cdots h_m(x)^{2^s - \sigma_m} h_1^*(x)^{2^s - \delta_1} \cdots h_m^*(x)^{2^s - \delta_m}.$$

Therefore it is obvious to see that the following theorem holds.

Theorem 5.1. *With the above notations, we have that C is self-dual if and only if* $2\tau_i = 2^s$ *for* $1 \leq i \leq n$, *and* $\delta_j + \sigma_j = 2^s$ *for* $1 \leq j \leq m$.

Recall the irreducible factorization of $x^{p_1 p_2^t p^s} - 1$ given in Corollary 3.2. Now we determine for each irreducible factor its reciprocal polynomial.

Lemma 5.1. *Let the notations be defined as Corollary 3.1. Then one of the following holds.*

(1) If both f_1 *and* f_2 *are odd, then we have that*

$$C_0^* = C_0,\ C^*_{\mu_1^k p_2^t} = C_{-\mu_1^k p_2^t},\ C^*_{\mu_2^{k'} p_1 p_2^r} = C_{-\mu_2^{k'} p_1 p_2^r},\ C^*_{\mu_1^{k_1} \mu_2^{k_2} p_2^r} = C_{-\mu_1^{k_1} \mu_2^{k_2} p_2^r}.$$

(2) If f_1 *is odd and* f_2 *is even, then we have that*

$$C_0^* = C_0,\ C^*_{\mu_1^k p_2^t} = C_{-\mu_1^k p_2^t},\ C^*_{\mu_2^{k'} p_1 p_2^r} = C_{\mu_2^{k'} p_1 p_2^r},\ C^*_{\mu_1^{k_1} \mu_2^{k_2} p_2^r} = C_{-\mu_1^{k_1} \mu_2^{k_2} p_2^r}.$$

(3) If f_1 *is even and* f_2 *is odd, then we have that*

$$C_0^* = C_0,\ C^*_{\mu_1^k p_2^t} = C_{\mu_1^k p_2^t},\ C^*_{\mu_2^{k'} p_1 p_2^r} = C_{-\mu_2^{k'} p_1 p_2^r},\ C^*_{\mu_1^{k_1} \mu_2^{k_2} p_2^r} = C_{-\mu_1^{k_1} \mu_2^{k_2} p_2^r}.$$

(4) If both f_1 and f_2 are even ,then we have when $v_2(f_1) \neq v_2(f_2)$,

$$C_0^* = C_0,\ C^*_{\mu_1^k p_2^t} = C_{\mu_1^k p_2^t},\ C^*_{\mu_2^{k'} p_1 p_2^r} = C_{\mu_2^{k'} p_1 p_2^r},\ C^*_{\mu_1^{k_1}\mu_2^{k_2} p_2^r} = C_{-\mu_1^{k_1}\mu_2^{k_2} p_2^r},$$

when $v_2(f_1) = v_2(f_2)$,

$$C_0^* = C_0,\ C^*_{\mu_1^k p_2^t} = C_{\mu_1^k p_2^t},\ C^*_{\mu_2^{k'} p_1 p_2^r} = C_{\mu_2^{k'} p_1 p_2^r},\ C^*_{\mu_1^{k_1}\mu_2^{k_2} p_2^r} = C_{-\mu_1^{k_1}\mu_2^{k_2} p_2^r}.$$

Proof. First it is trivial that the reciprocal of C_0 is always itself. For $C_{\mu_1^k p_2^t}$, notice that $C^*_{\mu_1^k p_2^t} = C_{\mu_1^k p_2^t}$ if and only if the congruence equation $-\mu_1^k p_2^t \equiv -\mu_1^k p_2^t q^x \pmod{p_1 p_2^t}$ is solvable. Since the equation is equivalent to $-1 \equiv q^x \pmod{p_2^r}$, then the condition holds if and only if $f_1 = \mathrm{ord}_{p_1}(q)$ is even. In the similar way we can check that $C^*_{\mu_2^{k'} p_1 p_2^r} = C_{\mu_2^{k'} p_1 p_2^r}$ if and only if $f_{2,t-r} = f_2 p_2^{max\{0,t-r\}}$ is even. Notice that by assumption p_2 is odd, therefore the condition holds if and only if f_2 is even. For $C_{\mu_1^{k_1}\mu_2^{k_2} p_2^r}$, consider the congruence equation $-\mu_1^{k_1}\mu_2^{k_2} p_2^r \equiv \mu_1^{k_1}\mu_2^{k_2} p_2^r q^x \pmod{p_1 p_2^t}$. It is equivalent to that $-1 \equiv q^x \pmod{p_1}$ and $-1 \equiv q^x \pmod{p_2^{t-r}}$ holds simultaneously. This requires not only both f_1 and f_2 are even, but also $\gcd(f_1, f_{2,t-r}) \mid \dfrac{f_1 - f_{2,t-r}}{2}$. And it is trivial to check that the last condition holds if and only if $v_2(f_1) = v_2(f_{2,t-r}) = v_2(f_2)$. □

Based on the above lemma, we now determine all the self-dual cyclic codes of length $p_1 p_2^t$ and their enumeration.

Theorem 5.2.

(1) If both f_1 and f_2 are odd, then there exist $(2^s + 1)^{\frac{p_1 p_2^t - 1}{2}}$ self-dual cyclic codes of length $p_1 p_2^t$ over $\mathbb{F}_{2^k}$, which are given by

$$\Big((x-1)^{2^{s-1}} \prod_{r=0}^{t-1} \prod_{k_1=0}^{\frac{g_1}{2}-1} \prod_{k_2=0}^{g_{2,t-r}\gcd(f_1,f_{2,t-r})-1} C_{\mu_1^{k_1}\mu_2^{k_2} p_2^r}(x)^{v_{\mu_1^{k_1}\mu_2^{k_2} p_2^r}} C_{-\mu_1^{k_1}\mu_2^{k_2} p_2^r}(x)^{2^s - v_{\mu_1^{k_1}\mu_2^{k_2} p_2^r}}$$
$$\cdot \prod_{k=0}^{\frac{g_1}{2}-1} C_{\mu_1^k p_2^t}(x)^{w_{\mu_1^k p_2^t}} C_{-\mu_1^k p_2^t}(x)^{2^s - w_{\mu_1^k p_2^t}} \prod_{r=0}^{t-1} \prod_{k'=0}^{\frac{g_{2,t-r}\gcd(f_1,f_{2,t-r})}{2}-1} C_{\mu_2^{k'} p_1 p_2^r}(x)^{x_{\mu_2^{k'} p_1 p_2^r}} C_{-\mu_2^{k'} p_1 p_2^r}(x)^{2^s - x_{\mu_2^{k'} p_1 p_2^r}}\Big).$$

(2) If f_1 is odd and f_2 is even, then there exist $(2^s + 1)^{\frac{p_1(p_2^t - 1)}{2}}$ self-dual cyclic codes of length $p_1 p_2^t$ over $\mathbb{F}_{2^k}$, which are given by

$$\Big((x-1)^{2^{s-1}} \prod_{r=0}^{t-1} \prod_{k_1=0}^{\frac{g_1}{2}-1} \prod_{k_2=0}^{g_{2,t-r}\gcd(f_1,f_{2,t-r})-1} C_{\mu_1^{k_1}\mu_2^{k_2} p_2^r}(x)^{v_{\mu_1^{k_1}\mu_2^{k_2} p_2^r}} C_{-\mu_1^{k_1}\mu_2^{k_2} p_2^r}(x)^{2^s - v_{\mu_1^{k_1}\mu_2^{k_2} p_2^r}}$$
$$\cdot \prod_{k=0}^{\frac{g_1}{2}-1} C_{\mu_1^k p_2^t}(x)^{w_{\mu_1^k p_2^t}} C_{-\mu_1^k p_2^t}(x)^{2^s - w_{\mu_1^k p_2^t}} \prod_{r=0}^{t-1} \prod_{k'=0}^{g_{2,t-r}\gcd(f_1,f_{2,t-r})-1} C_{\mu_2^{k'} p_1 p_2^r}(x)^{2^{s-1}}\Big).$$

(3) If f_1 is even and f_2 is odd, then there exist $(2^s + 1)^{\frac{p_2^t(p_1 - 1)}{2}}$ self-dual cyclic codes of length $p_1 p_2^t$ over $\mathbb{F}_{2^m}$, which are given by

$$\Big((x-1)^{2^{s-1}} \prod_{r=0}^{t-1} \prod_{k_1=0}^{g_1-1} \prod_{k_2=0}^{\frac{g_{2,t-r}\gcd(f_1,f_{2,t-r})}{2}-1} C_{\mu_1^{k_1}\mu_2^{k_2} p_2^r}(x)^{v_{\mu_1^{k_1}\mu_2^{k_2} p_2^r}} C_{-\mu_1^{k_1}\mu_2^{k_2} p_2^r}(x)^{2^s - v_{\mu_1^{k_1}\mu_2^{k_2} p_2^r}}$$
$$\cdot \prod_{k=0}^{g_1-1} C_{\mu_1^k p_2^t}(x)^{2^{s-1}} \prod_{r=0}^{t-1} \prod_{k'=0}^{\frac{g_{2,t-r}\gcd(f_1,f_{2,t-r})}{2}-1} C_{\mu_2^{k'} p_1 p_2^r}(x)^{x_{\mu_2^{k'} p_1 p_2^r}} C_{-\mu_2^{k'} p_1 p_2^r}(x)^{2^s - x_{\mu_2^{k'} p_1 p_2^r}}\Big).$$

(4) If both f_1 and f_2 are even ,then we have when $v_2(f_1) \neq v_2(f_2)$, there exist $(2^s+1)^{\frac{(p_1-1)(p_2^t-1)}{2}}$ self-dual cyclic codes of length $p_1p_2^t$ over $\mathbb{F}_{2^m}$, which are given by

$$\Big((x-1)^{2^{s-1}} \prod_{r=0}^{t-1} \prod_{k_1=0}^{g_1-1} \prod_{k_2=0}^{\frac{g_{2,t-r}\gcd(f_1,f_2,t-r)}{2}-1} C_{\mu_1^{k_1}\mu_2^{k_2}p_2^r}(x)^{v_{\mu_1^{k_1}\mu_2^{k_2}p_2^r}} C_{-\mu_1^{k_1}\mu_2^{k_2}p_2^r}(x)^{2^s-v_{\mu_1^{k_1}\mu_2^{k_2}p_2^r}}$$
$$\cdot \prod_{k=0}^{g_1-1} C_{\mu_1^k p_2^t}(x)^{2^{s-1}} \prod_{r=0}^{t-1} \prod_{k'=0}^{g_{2,t-r}\gcd(f_1,f_{2,t-r})-1} C_{\mu_2^{k'}p_1p_2^r}(x)^{2^{s-1}}\Big).$$

When $v_2(f_1) = v_2(f_2)$, there exist only one self-dual cyclic codes of length $p_1p_2^t$ over $\mathbb{F}_{2^m}$, which is given by

$$\Big((x-1)^{2^{s-1}} \prod_{r=0}^{t-1} \prod_{k_1=0}^{g_1-1} \prod_{k_2=0}^{g_{2,t-r}\gcd(f_1,f_{2,t-r})-1} C_{\mu_1^{k_1}\mu_2^{k_2}p_2^r}(x)^{2^{s-1}}$$
$$\cdot \prod_{k=0}^{g_1-1} C_{\mu_1^k p_2^t}(x)^{2^{s-1}} \prod_{r=0}^{t-1} \prod_{k'=0}^{g_{2,t-r}\gcd(f_1,f_{2,t-r})-1} C_{\mu_2^{k'}p_1p_2^r}(x)^{2^{s-1}}\Big).$$

6. Constacyclic codes of length $5\ell p^s$ over $\mathbb{F}_q$

In this section, we illustrate the above process with the example of constacyclic codes of length $5\ell p^s$, where ℓ is a prime number different from 5 and p. We determine all the constacyclic codes of length $5\ell p^s$ and their dual codes over $\mathbb{F}_q$, and then all the self-dual codes of length $5\ell p^s$ are also given.

First we determine all the q-cyclotomic cosets modulo 5ℓ. Let $f = \mathrm{ord}_\ell(q)$, and $e = \dfrac{\ell-1}{f}$. Then we have:
(1) $\mathrm{ord}_{5\ell}(q) = f$, when $q \equiv 1 \pmod 5$.
(2) $\mathrm{ord}_{5\ell}(q) = f$, when $q \equiv 4 \pmod 5$ with f even.
(3) $\mathrm{ord}_{5\ell}(q) = 2f$, when $q \equiv 4 \pmod 5$ with f odd.
(4) $\mathrm{ord}_{5\ell}(q) = f$, when $q \equiv 2$ or $q \equiv 3 \pmod 5$ with $4 \mid f$.
(5) $\mathrm{ord}_{5\ell}(q) = 2f$, when $q \equiv 2$ or $q \equiv 3 \pmod 5$ with $2 \mid f$ but $4 \nmid f$.
(6) $\mathrm{ord}_{5\ell}(q) = 4f$, when $q \equiv 2$ or $q \equiv 3 \pmod 5$ with f odd.

As the discussion given in the Section 3, we can find a primitive root μ modulo ℓ^t for all $t \geq 1$ such that $\mu \equiv 1 \pmod 5$. The following lemma give more explicit formula for the q-cyclotomic cosets modulo 5ℓ.

Lemma 6.1.

(1) If $q \equiv 1 \pmod 5$, then we have that all the distinct q-cyclotomic cosets modulo 5ℓ are given by $C_0 = \{0\}$, $C_\ell = \{\ell\}$, $C_{2\ell} = \{2\ell\}$, $C_{-\ell} = \{-\ell\}$, $C_{-2\ell} = \{-2\ell\}$, and $C_{a\mu^k} = \{a\mu^k, a\mu^k q, \cdots, a\mu^k q^{f-1}\}$ for $a \in R = \{1, 2, -1, -2, 5\}$ and $0 \leq k \leq e-1$.

(2) If $q \equiv 4 \pmod 5$ and f is even, we have that all the distinct q-cyclotomic cosets modulo 5ℓ are given by $C_0 = \{0\}$, $C_\ell = \{\ell, \ell q\}$, $C_{2\ell} = \{2\ell, 2\ell q\}$, $C_{\mu^{k'}} = \{\mu^{k'}, \mu^{k'}q, \cdots, \mu^{k'}q^{f-1}\}$, $C_{2\mu^{k'}} = \{2\mu^{k'}, 2\mu^{k'}q, \cdots, 2\mu^{k'}q^{f-1}\}$ for $0 \leq k' \leq 2e-1$, and $C_{5\mu^k} = \{5\mu^k, 5\mu^k q, \cdots, 5\mu^k q^{f-1}\}$ for $0 \leq k \leq e-1$.

(3) If $q \equiv 4 \pmod 5$ and f is odd, we have that all the distinct q-cyclotomic cosets modulo 5ℓ are given by $C_0 = \{0\}$, $C_\ell = \{\ell, \ell q\}$, $C_{2\ell} = \{2\ell, 2\ell q\}$, $C_{\mu^k} = \{\mu^k, \mu^k q, \cdots, \mu^k q^{2f-1}\}$, $C_{2\mu^k} = \{2\mu^k, 2\mu^k q, \cdots, 2\mu^k q^{2f-1}\}$, and $C_{5\mu^k} = \{5\mu^k, 5\mu^k q, \cdots, 5\mu^k q^{f-1}\}$ for $0 \leq k \leq e-1$.

(4) *If* $q \equiv 2$ *or* $3 \pmod 5$ *and* $4 \mid f$, *we have that all the distinct q-cyclotomic cosets modulo* 5ℓ *are given by* $C_0 = \{0\}$, $C_\ell = \{\ell, \ell q, \ell q^2, \ell q^3\}$, $C_{\mu^{k'}} = \{\mu_{k'}, \mu^{k'}q, \cdots, \mu^{k'}q^{f-1}\}$ *for* $0 \leq k' \leq 4e-1$, *and* $C_{5\mu^k} = \{5\mu^k, 5\mu^k q, \cdots, 5\mu^k q^{f-1}\}$ *for* $0 \leq k \leq e-1$.

(5) *If* $q \equiv 2$ *or* $3 \pmod 5$ *and* $2 \mid f$ *but* $4 \nmid f$, *we have that all the distinct q-cyclotomic cosets modulo* 5ℓ *are given by* $C_0 = \{0\}$, $C_\ell = \{\ell, \ell q, \ell q^2, lq^3\}$, $C_{\mu^{k'}} = \{\mu_{k'}, \mu^{k'}q, \cdots, \mu^{k'}q^{2f-1}\}$ *for* $0 \leq k' \leq 2e-1$, *and* $C_{5\mu^k} = \{5\mu^k, 5\mu^k q, \cdots, 5\mu^k q^{f-1}\}$ *for* $0 \leq k \leq e-1$.

(6) *If* $q \equiv 2$ *or* $3 \pmod 5$ *and f is odd, we have that all the distinct q-cyclotomic cosets modulo* 5ℓ *are given by* $C_0 = \{0\}$, $C_\ell = \{\ell, \ell q, \ell q^2, \ell q^3\}$, $C_{\mu^k} = \{\mu_k, \mu^k q, \cdots, \mu^k q^{4f-1}\}$, *and* $C_{5\mu^k} = \{5\mu^k, 5\mu^k q, \cdots, 5\mu^k q^{f-1}\}$ *for* $0 \leq k \leq e-1$.

Proof. The methods to prove the above 6 situations are similar, and we will give the proof of the second situation as a instance. First since μ is a fixed primitive root modulo l such that $\mu \equiv 1 \pmod 5$, it is trivial to verify that C_0, C_ℓ, $C_{2\ell}$, $C_{\mu^{k'}}$, $C_{2\mu^{k'}}$ for $0 \leq k' \leq 2e-1$ and $C_{5\mu^k}$ for $0 \leq k \leq e-1$ are q-cyclotomic cosets modulo 5ℓ. And then we claim that all these cosets are all distinct. If we have that $a_1\mu^{k_1} \equiv a_2\mu^{k_2}q^j$, where a_1, a_2, k_1, k_2 and j satisfy the definitions in (2). Since

$$\gcd(a_1, 5\ell) = \gcd(a_1\mu^{k_1}, 5\ell) = \gcd(a_2\mu^{k_2}q^j, 5\ell) = \gcd(a_2, 5\ell),$$

we have that either $a_1 = a_2$ or $a_1 \neq a_2$ and both a_1 and a_2 are not equal to 5. We divide the proof into 2 subcases.

Subcase 1. If $a_1 = a_2$, we have that $\mu^{k_1-k_2} \equiv q^j \pmod \ell$ and $\mu^{(k_1-k_2)f} \equiv 1 \pmod \ell$, therefore $\phi(\ell) \mid (k_1-k_2)f$ and $\frac{\phi(\ell)}{f} \mid (k_1-k_2)$, which indicates that $k_1 = k_2$.

Subcase 2. If $a_1 \neq a_2$ and none of them is equal to 5, we have that $a_1a_2^{-1} \equiv \mu^{k_2-k_1}q^j \pmod{5\ell}$, but notice that $a_1a_2^{-1} \equiv \pm 2 \pmod 5$ and $\mu^{k_2-k_1}q^j \equiv \pm 1 \pmod 5$, which is a contradiction. Hence the given cosets are all distinct, and we only need to prove they are all the q-cyclotomic cosets to complete the proof.

Notice that

$$|C_0| + |C_\ell| + |C_{2\ell}| + \sum_{k'=0}^{2e-1}|C_{\mu^{k'}}| + \sum_{k'=0}^{2e-1}|C_{2\mu^{k'}}| + \sum_{k=0}^{e-1}|C_{5\mu^k}| = 5 + 2ef + 2ef + ef = 5(ef+1) = 5(\phi(\ell)+1) = 5\ell.$$

Therefore the conclusion holds. □

Theorem 6.1. *The irreducible factorization of* $x^{5\ell} - 1$ *over* $\mathbb{F}_q$ *is given as follows.*

(1) *If* $q \equiv 1 \pmod 5$, *then*

$$x^{5\ell} - 1 = C_0(x)C_\ell(x)C_{2\ell}(x)C_{3\ell}(x)C_{4\ell}(x)\prod_{a\in R}\prod_{k=0}^{e-1} C_{a\mu^k}(x),$$

where $R = 1, 2, 3, 4, 5$.

(2) *If* $q \equiv 4 \pmod 5$ *and f is even, then*

$$x^{5\ell} - 1 = C_0(x)C_\ell(x)C_{2\ell}(x)\prod_{k'=0}^{2e-1} C_{\mu^{k'}}(x)C_{2\mu^{k'}}(x)\prod_{k=0}^{e-1} C_{5\mu^k}(x),$$

(3) If $q \equiv 4 \pmod 5$ and f is odd, then

$$x^{5\ell} - 1 = C_0(x)C_\ell(x)C_{2\ell}(x)\prod_{k=0}^{e-1} C_{\mu^k}(x)C_{2\mu^k}(x)C_{5\mu^k}(x),$$

(4) If $q \equiv 2$ or $3 \pmod 5$ and $4 \mid f$, then

$$x^{5\ell} - 1 = C_0(x)C_\ell(x)\prod_{k'=0}^{4e-1} C_{\mu^{k'}}(x)\prod_{k=0}^{e-1} C_{5\mu^k}(x),$$

(5) If $q \equiv 2$ or $3 \pmod 5$ and $2 \mid f$ but $4 \nmid f$, then

$$x^{5\ell} - 1 = C_0(x)C_\ell(x)\prod_{k'=0}^{2e-1} C_{\mu^{k'}}(x)\prod_{k=0}^{e-1} C_{5\mu^k}(x),$$

(6) If $q \equiv 2$ or $3 \pmod 5$ and f is odd, then

$$x^{5\ell} - 1 = C_0(x)C_\ell(x)\prod_{k=0}^{e-1} C_{\mu^k}(x)C_{5\mu^k}(x),$$

With the irreducible factorization of $x^{5\ell} - 1$, we can straightly follow the process given in Section 4 to calculate all the constacyclic codes of length $5\ell p^s$ over $\mathbb{F}_q$. We list the result as follow.

Theorem 6.2. *Assume that $\gcd(q-1, 5\ell p^s) = 1$, then λ-constacyclic codes C of length $5\ell p^s$ over $\mathbb{F}_q$ are equivalent to the cyclic codes, i.e., for any $\lambda \in \mathbb{F}_q^*$, there exists a unique element $a \in \mathbb{F}_q^*$ such that $a^{5\ell p^s}\lambda = 1$. Furthermore, the irreducible factorization of $x^{5\ell p^s} - \lambda$ over $\mathbb{F}_q$ is given by*

(1) If $q \equiv 4 \pmod 5$ and f is even, then

$$x^{5\ell p^s} - \lambda = \widehat{C}_0(ax)^{p^s}\widehat{C}_\ell(ax)^{p^s}\widehat{C}_{2\ell}(ax)^{p^s}\prod_{k'=0}^{2e-1}\widehat{C}_{\mu^{k'}}(ax)^{p^s}\widehat{C}_{2\mu^{k'}}(ax)^{p^s}\prod_{k=0}^{e-1}\widehat{C}_{5\mu^k}(ax)^{p^s},$$

Therefore we have that

$$C = \left(\widehat{C}_0(ax)^{\varepsilon_1}\widehat{C}_\ell(ax)^{\varepsilon_2}\widehat{C}_{2\ell}(ax)^{\varepsilon_3}\prod_{k'=0}^{2e-1}\widehat{C}_{\mu^{k'}}(ax)^{\tau_{k'}}\widehat{C}_{2\mu^{k'}}(ax)^{\nu_{k'}}\prod_{k=0}^{e-1}\widehat{C}_{5\mu^k}(ax)^{\rho_k}\right),$$

and

$$\begin{aligned} C^\perp \;=\; & \Big(\widehat{C}_0(a^{-1}x)^{p^s-\varepsilon_1}\widehat{C}_{-\ell}(a^{-1}x)^{p^s-\varepsilon_2}\widehat{C}_{-2\ell}(a^{-1}x)^{p^s-\varepsilon_3} \\ & \times\prod_{k'=0}^{2e-1}\widehat{C}_{-\mu^{k'}}(a^{-1}x)^{p^s-\tau_{k'}}\widehat{C}_{-2\mu^{k'}}(a^{-1}x)^{p^s-\nu_{k'}}\prod_{k=0}^{e-1}\widehat{C}_{-5\mu^k}(a^{-1}x)^{p^s-\rho_k}\Big), \end{aligned}$$

where $0 \le \varepsilon_1, \varepsilon_2, \varepsilon_3, \tau_{k'}, \nu_{k'}, \rho_k \le p^s$, for any $k' = 0, 1, \cdots, 2e-1$, and $k = 0, 1, \cdots, e-1$.

(2) If $q \equiv 4 \pmod{5}$ and f is odd, then

$$x^{5\ell p^s} - \lambda = \widehat{C}_0(ax)^{p^s}\widehat{C}_\ell(ax)^{p^s}\widehat{C}_{2\ell}(ax)^{p^s}\prod_{k=0}^{e-1}\widehat{C}_{\mu^k}(ax)^{p^s}\widehat{C}_{2\mu^k}(ax)^{p^s}\widehat{C}_{5\mu^k}(ax)^{p^s}.$$

Therefore we have that

$$C = \left(\widehat{C}_0(ax)^{\varepsilon_1}\widehat{C}_\ell(ax)^{\varepsilon_2}\widehat{C}_{2\ell}(ax)^{\varepsilon_3}\prod_{k=0}^{e-1}\widehat{C}_{\mu^k}(ax)^{\tau_k}\widehat{C}_{2\mu^k}(ax)^{\nu_k}\widehat{C}_{5\mu^k}(ax)^{\rho_k}\right),$$

and

$$\begin{aligned} C^{\perp} &= \Big(\widehat{C}_0(a^{-1}x)^{p^s-\varepsilon_1}\widehat{C}_{-\ell}(a^{-1}x)^{p^s-\varepsilon_2}\widehat{C}_{-2\ell}(a^{-1}x)^{p^s-\varepsilon_3} \\ &\quad \times \prod_{k=0}^{e-1}\widehat{C}_{-\mu^k}(a^{-1}x)^{p^s-\tau_k}\widehat{C}_{-2\mu^k}(a^{-1}x)^{p^s-\nu_k}\widehat{C}_{-5\mu^k}(a^{-1}x)^{p^s-\rho_k}\Big), \end{aligned}$$

where $0 \le \varepsilon_1, \varepsilon_2, \varepsilon_3, \tau_k, \nu_k, \rho_k \le p^s$, for $k = 0, 1, \cdots, e-1$.

(3) If $q \equiv 2$ or $3 \pmod{5}$ and $4 \mid f$, then

$$x^{5\ell p^s} - \lambda = \widehat{C}_0(ax)^{p^s}\widehat{C}_\ell(ax)^{p^s}\prod_{k'=0}^{4e-1}\widehat{C}_{\mu^{k'}}(ax)^{p^s}\prod_{k=0}^{e-1}\widehat{C}_{5\mu^k}(ax)^{p^s}.$$

Therefore we have that

$$C = \left(\widehat{C}_0(ax)^{\varepsilon_1}\widehat{C}_\ell(ax)^{\varepsilon_2}\prod_{k'=0}^{4e-1}\widehat{C}_{\mu^{k'}}(ax)^{\tau_{k'}}\prod_{k=0}^{e-1}\widehat{C}_{5\mu^k}(ax)^{\nu_k}\right),$$

and

$$C^{\perp} = \left(\widehat{C}_0(a^{-1}x)^{p^s-\varepsilon_1}\widehat{C}_{-\ell}(a^{-1}x)^{p^s-\varepsilon_2}\prod_{k'=0}^{4e-1}\widehat{C}_{-\mu^{k'}}(a^{-1}x)^{p^s-\tau_{k'}}\prod_{k=0}^{e-1}\widehat{C}_{-5\mu^k}(a^{-1}x)^{p^s-\nu_k}\right),$$

where $0 \le \varepsilon_1, \varepsilon_2, \tau_{k'}, \nu_k \le p^s$, for $k^{'} = 0, 1, \cdots, 4e-1$, and $k = 0, 1, \cdots, e-1$.

(4) If $q \equiv 2$ or $3 \pmod{5}$ and $2 \mid f$ but $4 \nmid f$, then

$$x^{5\ell p^s} - \lambda = \widehat{C}_0(ax)^{p^s}\widehat{C}_\ell(ax)^{p^s}\prod_{k'=0}^{2e-1}\widehat{C}_{\mu^{k'}}(ax)^{p^s}\prod_{k=0}^{e-1}\widehat{C}_{5\mu^k}(ax)^{p^s}.$$

Therefore we have that

$$C = \left(\widehat{C}_0(ax)^{\varepsilon_1}\widehat{C}_\ell(ax)^{\varepsilon_2}\prod_{k'=0}^{2e-1}\widehat{C}_{\mu^{k'}}(ax)^{\tau_{k'}}\prod_{k=0}^{e-1}\widehat{C}_{5\mu^k}(ax)^{\nu_k}\right),$$

and

$$C^{\perp} = \left(\widehat{C}_0(a^{-1}x)^{p^s-\varepsilon_1}\widehat{C}_{-\ell}(a^{-1}x)^{p^s-\varepsilon_2}\prod_{k'=0}^{2e-1}\widehat{C}_{-\mu^{k'}}(a^{-1}x)^{p^s-\tau_{k'}}\prod_{k=0}^{e-1}\widehat{C}_{-5\mu^k}(a^{-1}x)^{p^s-\nu_k}\right),$$

where $0 \le \varepsilon_1, \varepsilon_2, \tau_{k'}, \nu_k \le p^s$, for $k^{'} = 0, 1, \cdots, 2e-1$, and $k = 0, 1, \cdots, e-1$.

(5) If $q \equiv 2$ *or* $3 \pmod 5$ *and* f *is odd, then*

$$x^{5\ell p^s} - \lambda = \widehat{C}_0(ax)^{p^s}\widehat{C}_\ell(ax)^{p^s}\prod_{k=0}^{e-1}\widehat{C}_{\mu^k}(ax)^{p^s}\widehat{C}_{5\mu^k}(ax)^{p^s}.$$

Therefore we have that

$$C = \left(\widehat{C}_0(ax)^{\varepsilon_1}\widehat{C}_\ell(ax)^{\varepsilon_2}\prod_{k=0}^{e-1}\widehat{C}_{\mu^k}(ax)^{\tau_k}\widehat{C}_{5\mu^k}(ax)^{\nu_k}\right),$$

and

$$C^\perp = \left(\widehat{C}_0(a^{-1}x)^{p^s-\varepsilon_1}\widehat{C}_{-\ell}(a^{-1}x)^{p^s-\varepsilon_2}\prod_{k=0}^{e-1}\widehat{C}_{-\mu^k}(a^{-1}x)^{p^s-\tau_k}\widehat{C}_{-5\mu^k}(a^{-1}x)^{p^s-\nu_k}\right),$$

where $0 \le \varepsilon_1, \varepsilon_2, \tau_k, \nu_k \le p^s$, *for* $k = 0, 1, \cdots, e-1$.

Theorem 6.3. *Assume that* $\gcd(q-1, 5\ell p^s) = 5\ell$, *then* $\mathbb{F}_q^* = \langle\xi\rangle = \langle\xi^{5\ell}\rangle \cup \langle\xi^{5\ell}\rangle\xi^{p^s} \cup \cdots \cup \langle\xi^{5\ell}\rangle\xi^{p^s(5\ell-1)}$. *For any* $\lambda \in \mathbb{F}_q^*$, *there exists an element* $a \in \mathbb{F}_q^*$ *such that* $a^{5\ell p^s}\lambda = \xi^{j\cdot p^s}$, *where* $0 \le j \le 5\ell - 1$. *Then* j *can be written as* $j = y \cdot 5^{v_1}\ell^{v_2}$, *where* $v_1 = \min\{1, v_5(j)\}$ *and* $v_2 = \min\{1, v_\ell(j)\}$. *And*

$$\begin{aligned} x^n - \lambda &= (x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\xi^y)^{p^s}(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta\xi^y)^{p^s} \\ &\quad \cdots (x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta^{5^{v_1}\ell^{v_2}-1}\xi^y)^{p^s} \end{aligned}$$

gives the irreducible factorization of $x^{5\ell p^s} - \lambda$ *over* $\mathbb{F}_q$. *Moreover, all the* λ*-constacyclic codes of length* $5lp^s$ *and their dual codes are given by*

$$\begin{aligned} C &= \Big((x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\xi^y)^{\varepsilon_1}(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta\xi^y)^{\varepsilon_2} \\ &\quad \cdots (x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta^{5^{v_1}\ell^{v_2}-1}\xi^y)^{\varepsilon_{5^{v_1}\ell^{v_2}}}\Big), \end{aligned}$$

and

$$\begin{aligned} C^\perp &= \Big((x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}}\xi^{-y})^{p^s-\varepsilon_1}(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}}\delta^{-1}\xi^{-y})^{p^s-\varepsilon_2} \\ &\quad \cdots (x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}}\delta^{1-5^{v_1}\ell^{v_2}}\xi^{-y})^{p^s-\varepsilon_{5^{v_1}\ell^{v_2}}}\Big), \end{aligned}$$

where $0 \le \varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{5^{v_1}\ell^{v_2}} \le p^s$.

Theorem 6.4. *Assume that* $\gcd(q-1, 5\ell p^s) = 5$, *then for any* $0 \le j \le 4$, *there exists an element* $a \in \mathbb{F}_{q^f}*$ *such that* $a^{5\ell p^s}\xi^{j\cdot p^s} = \zeta^{j'\cdot p^s}$. *Moreover, each irreducible factor of* $x^{5\ell} - \xi^j$ *over* $\mathbb{F}_q$ *is of the form*

$$\begin{aligned} &(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'})(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{iq}\zeta^{y'q}) \\ &\cdots (x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y'q^{z_i-1}}), \end{aligned}$$

where $j' = y'5^{v_1}\ell^{v_2}$, $v_1 = \min\{1, v_5(j')\}$, $v_2 = \min\{1, v_\ell(j')\}$, *and* z_i *is the least positive integer such that* $a^{-q^{z_i}5^{1-v_1}\ell^{1-v_2}}\delta^{iq^{z_i}}\zeta^{y'q^{z_i}} = a^{5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'}$.

For any $0 \leq i, i^{'} \leq 5^{v_1}\ell^{v_2} - 1$, we define a relation $\sim$ to be such that $i \sim i^{'}$ if and only if $a^{-q^m 5^{1-v_1}\ell^{1-v_2}}\delta^{iq^m}\zeta^{y' q^m} = a^{5^{1-v_1}\ell^{1-v_2}}\delta^{i^{'}}\zeta^{y'}$ for some nonnegative integers m. It is obvious to see that $\sim$ is an equivalence relation. Assume that S is a complete system of equivalence class representatives of $\{0, 1, \cdots, 5^{v_1}\ell^{v_2} - 1\}$ relative to this relation $\sim$. For any $i \in S$ we denote the irreducible polynomial

$$\begin{aligned}&(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'})(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{iq}\zeta^{y'q})\\ &\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y' q^{z_i-1}}),\end{aligned}$$

by $M_i(x)$, and denote

$$\begin{aligned}&(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}}\delta^{-i}\zeta^{-y'})(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{-iq}\zeta^{-y'q})\\ &\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{-iq^{z_i-1}}\zeta^{-y' q^{z_i-1}}),\end{aligned}$$

by $M_i^{'}(x)$. Then we have the following corollary.

Corollary 6.1. *Assume that* $\gcd(q-1, 5\ell p^s) = 5$. *For any* $0 \leq j \leq 4$, *there exists an element* $a \in \mathbb{F}_{q^f}*$ *such that* $a^{5\ell p^s}\xi^{j\cdot p^s} = \zeta^{j'\cdot p^s}$. *Then*

$$x^{5\ell p^s} - \xi^{jp^s} = \prod_{i\in S} M_i(x)^{p^s}$$

gives the irreducible factorization of $x^{5\ell p^s} - \xi^{jp^s}$ *over* $\mathbb{F}_q$. *Furthermore we have that*

$$C = \left\langle \prod_{i\in X} M_i(x)^{\varepsilon_i} \right\rangle,$$

and

$$C^{\perp} = \left\langle \prod_{i\in X} M_i^{'}(x)^{p^s-\varepsilon_i} \right\rangle,$$

where $0 \leq \varepsilon_i \leq p^s$, *for* $i \in X$.

Theorem 6.5. *Assume that* $\gcd(q-1, 5\ell p^s) = \ell$, *then*

(1) If $q \equiv 4 \pmod 5$, *for any* $0 \leq j \leq \ell - 1$, *the following equations*

$$j' \equiv 2j \pmod \ell \text{ and } j' \equiv 0 \pmod 5$$

have a unique solution j' *up to modulo* 5ℓ. *Moreover, each irreducible facotor of* $x^{5\ell} - \xi^j$ *over* $\mathbb{F}_q$ *is of the form*

$$\begin{aligned}&(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'})(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{iq}\zeta^{y'q})\\ &\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y' q^{z_i-1}}),\end{aligned}$$

where $j' = y'5^{v_1}\ell^{v_2}$, $v_1 = \min\{1, v_5(j')\}$, $v_2 = \min\{1, v_\ell(j')\}$, *and* z_i *is the least positive integer such that* $a^{-q^{z_i}5^{1-v_1}\ell^{1-v_2}}\delta^{iq^{z_i}}\zeta^{y' q^{z_i}} = a^{5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'}$.

(2) If $q \equiv 2, 3 \pmod 5$, *for any* $0 \leq j \leq \ell - 1$, *the following equations*

$$j' \equiv 4j \pmod \ell$$

$$j' \equiv 0 \pmod 5$$

have a unique solution j' up to modulo 5ℓ. Moreover, each irreducible facotor of $x^{5\ell} - \xi^j$ over $\mathbb{F}_q$ is of the form

$$(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'})(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{iq}\zeta^{y'q})$$
$$\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y'q^{z_i-1}}),$$

where $j' = y'5^{v_1}\ell^{v_2}$, $v_1 = min1, v_5(j')$, $v_2 = min1, v_\ell(j')$, and z_i is the least positive integer such that $a^{-q^{z_i}5^{1-v_1}\ell^{1-v_2}}\delta^{iq^{z_i}}\zeta^{y'q^{z_i}} = a^{5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'}$.

For any $0 \leq i, i' \leq 5^{v_1}\ell^{v_2} - 1$, we define a relation $\sim$ to be such that $i \sim i'$ if and only if $a^{-q^m 5^{1-v_1}\ell^{1-v_2}}\delta^{iq^m}\zeta^{y'q^m} = a^{5^{1-v_1}\ell^{1-v_2}}\delta^{i'}\zeta^{y'}$ for some nonnegative integer m. It is obvious to see that $\sim$ is an equivalence relation. Assume that S is a complete system of equivalence class representatives of $\{0, 1, \cdots, 5^{v_1}\ell^{v_2} - 1\}$ relative to this relation $\sim$. For any $i \in S$ we denote the irreducible polynomial

$$(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}}\delta^i\zeta^{y'})(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{iq}\zeta^{y'q})$$
$$\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - a^{-5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{iq^{z_i-1}}\zeta^{y'q^{z_i-1}}),$$

by $M_i(x)$, and denote

$$(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}}\delta^{-i}\zeta^{-y'})(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}\cdot q}\delta^{-iq}\zeta^{-y'q})$$
$$\cdots(x^{5^{1-v_1}\ell^{1-v_2}} - a^{5^{1-v_1}\ell^{1-v_2}\cdot q^{z_i-1}}\delta^{-iq^{z_i-1}}\zeta^{-y'q^{z_i-1}}),$$

by $M_i^{'}(x)$.

Corollary 6.2. *Assume that* $\gcd(q-1, 5\ell p^s) = \ell$*, then*

(1) If $q \equiv 4 \pmod 5$, and $j, j^{'}$ is defined as in the first case of Theorem 5.1, then

$$x^{5\ell p^s} - \xi^{jp^s} = \prod_{i\in X} M_i(x)^{p^s}$$

gives the irreducible factorization of $x^{5\ell p^s} - \xi^{jp^s}$ over $\mathbb{F}_q$. Furthermore we have that

$$C = \left(\prod_{i\in X} M_i(x)^{\varepsilon_i}\right),$$

and

$$C^{\perp} = \left(\prod_{i\in X} M_i^{'}(x)^{p^s-\varepsilon_i}\right),$$

where $0 \leq \varepsilon_i \leq p^s$, for $i \in X$.

(2) If $q \equiv 2, 3 \pmod 5$, and $j, j^{'}$ is defined as in the second case of Theorem 5.1, then

$$x^{5\ell p^s} - \xi^{jp^s} = \prod_{i\in X} M_i(x)^{p^s}$$

gives the irreducible factorization of $x^{5\ell p^s} - \xi^{jp^s}$ *over* $\mathbb{F}_q$. *Furthermore we have that*

$$C = \left(\prod_{i \in X} M_i(x)^{\varepsilon_i} \right),$$

and

$$C^{\perp} = \left(\prod_{i \in X} M_i^{'}(x)^{p^s - \varepsilon_i} \right),$$

where $0 \le \varepsilon_i \le p^s$, *for* $i \in X$.

Finally we give all the self-dual constacylic codes of length $5\ell p^s$ as the end of this section. Since self-dual cyclic codes of length N over $\mathbb{F}_q$ exists if and only if N is even and the characteristic of $\mathbb{F}_q$ is $p = 2$, as in the general case, we only consider the case of self-dual cyclic codes of length $5 \cdot 2^s \ell$ over $\mathbb{F}_{2^m}$.

Lemma 6.2. *Assume that* $q \equiv 1 \pmod 5$. *For the q-cyclotomic cosets, one of the following holds.*

(1) If $f = \mathrm{ord}_\ell(q)$ *is even, we have that*

$$C_0^* = C_0,\ C_\ell^* = C_{-\ell},\ C_{2\ell}^* = C_{-2\ell},\ C_{\mu^k}^* = C_{-\mu^k},\ C_{2\mu^k}^* = C_{-2\mu^k},\ C_{5\mu^k}^* = C_{5\mu^k},$$

where $0 \le k \le e - 1$.

(2) If $f = \mathrm{ord}_\ell(q)$ *is odd, we have that*

$$C_0^* = C_0,\ C_\ell^* = C_{-\ell},\ C_{2\ell}^* = C_{-2\ell},\ C_{\mu^k}^* = C_{-\mu^k},\ C_{2\mu^k}^* = C_{-2\mu^k},\ C_{5\mu^{k'}}^* = C_{-5\mu^{k'}},$$

where $\{C_{5\mu^k}\} = \{C_{5\mu^{k'}}\} \bigcup \{C_{-5\mu^{k'}}\}$, *and* $0 \le k \le e - 1$, $0 \le k' \le \dfrac{e}{2} - 1$.

Proof.

(1) By the definition of reciprocal coset, it is clear that $C_0^* = C_0$, $C_\ell^* = C_{-\ell}$, $C_{2\ell}^* = C_{-2\ell}$, $C_{\mu^k}^* = C_{-\mu^k}$, $C_{2\mu^k}^* = C_{-2\mu^k}$, thus it remains to prove $C_{5\mu^k}^* = C_{5\mu^k}$. Let $t = \frac{f}{2}$. Since $f = \mathrm{ord}_\ell(q)$, it is trivial to see that $q^t \equiv -1 \pmod \ell$, and therefore we have that $-5\mu^k \equiv 5\mu^k q^t \pmod{5\ell}$. It follows immediately that $C_{5\mu^k}^* = C_{5\mu^k}$, for $0 \le k \le e - 1$.

(2) As in the first case, the conclusions that $C_0^* = C_0$, $C_\ell^* = C_{-\ell}$, $C_{2\ell}^* = C_{-2\ell}$, $C_{\mu^k}^* = C_{-\mu^k}$, $C_{2\mu^k}^* = C_{-2\mu^k}$ are clear, and now we prove that $C_{5\mu^{k'}}^* = C_{-5\mu^{k'}}$. To see this, we claim that for any $0 \le k_1^{'}, k_2^{'} \le \frac{e}{2} - 1$, $C_{5\mu^{k_1^{'}}} \ne C_{-5\mu^{k_2^{'}}}$, and $\{C_{5\mu^k}\} = \{C_{5\mu^{k'}}\} \bigcup \{C_{-5\mu^{k'}}\}$. Assume that $C_{5\mu^{k_1^{'}}} = C_{-5\mu^{k_2^{'}}}$ for some $0 \le k_1^{'}, k_2^{'} \le \frac{e}{2} - 1$, then we have that $5\mu^{k_1^{'}} \equiv -5\mu^{k_2^{'}} q^j \pmod{5\ell}$ for some $0 \le j \le f - 1$, which indicates that $-\mu^{k_1^{'} - k_2^{'}} \equiv q^j \pmod \ell$. Notice that f is odd, therefore we have that $-\mu^{f(k_1^{'} - k_2^{'})} \equiv q^{jf} \equiv 1 \pmod \ell$ and $\mu^{f(k_1^{'} - k_2^{'})} \equiv -1 \pmod \ell$. It follows that $\mu^{2f(k_1^{'} - k_2^{'})} \equiv 1 \pmod \ell$, hence $\phi(\ell) \mid 2f(k_1^{'} - k_2^{'})$ and $\frac{e}{2} \mid k_1^{'} - k_2^{'}$. Since by the condition we have $0 \le k_1^{'}, k_2^{'} \le \frac{e}{2} - 1$, we deduce that $k_1^{'} = k_2^{'}$. Then the equation $5\mu^{k_1^{'}} \equiv -5\mu^{k_2^{'}} q^j \pmod{5\ell}$ can be reduced to $-1 \equiv q^j \pmod \ell$. However, notice that $\mathrm{ord}_\ell(q) = f$ is odd, such a positive integer j cannot exist, which is a contradiction. According to this, we have that for any $0 \le k_1^{'}, k_2^{'} \le \frac{e}{2} - 1$, $C_{5\mu^{k_1^{'}}} \ne C_{-5\mu^{k_2^{'}}}$. By comparing the number of elements, it is trivial to verify that $\{C_{5\mu^k}\} = \{C_{5\mu^{k'}}\} \bigcup \{C_{-5\mu^{k'}}\}$ holds. Then by the definition of reciprocal coset, one immediately get that $C_{5\mu^{k'}}^* = C_{-5\mu^{k'}}$. □

With the same method we can prove the results for the rest of cases. The proofs will be omitted.

Lemma 6.3. *Assume that* $q \equiv 4 \pmod 5$. *For the q-cyclotomic cosets, one of the following holds.*

(1) If $f = 2t$ *is even, then*

(i) when t is even, we have that

$$C_0^* = C_0,\ C_\ell^* = C_\ell,\ C_{2\ell}^* = C_{2\ell},\ C_{\mu^k}^* = C_{-\mu^k},\ C_{2\mu^k}^* = C_{-2\mu^k},\ C_{5\mu^k}^* = C_{5\mu^k},$$

where $\{C_{\mu^{k'}}\} = \{C_{\mu^k}\} \bigcup \{C_{-\mu^k}\}$, $\{C_{2\mu^{k'}}\} = \{C_{2\mu^k}\} \bigcup \{C_{-2\mu^k}\}$, *for* $0 \le k \le e-1$, $0 \le k^{'} \le 2e-1$.

(ii) If t is odd, we have that

$$C_0^* = C_0,\ C_\ell^* = C_\ell,\ C_{2\ell}^* = C_{2\ell},\ C_{\mu^{k'}}^* = C_{\mu^{k'}},\ C_{2\mu^{k'}}^* = C_{2\mu^{k'}},\ C_{5\mu^k}^* = C_{5\mu^k},$$

where $0 \le k \le e-1$, $0 \le k^{'} \le 2e-1$.

(2) when f is odd, then

$$C_0^* = C_0,\ C_\ell^* = C_\ell,\ C_{2\ell}^* = C_{2\ell},\ C_{\mu^{k'}}^* = C_{-\mu^{k'}},\ C_{2\mu^{k'}}^* = C_{-2\mu^{k'}},\ C_{5\mu^{k'}}^* = C_{-5\mu^{k'}},$$

where $\{C_{\mu^k}\} = \{C_{\mu^{k'}}\} \bigcup \{C_{-\mu^{k'}}\}$, $\{C_{2\mu^k}\} = \{C_{2\mu^{k'}}\} \bigcup \{C_{-2\mu^{k'}}\}$, $\{C_{5\mu^k}\} = \{C_{5\mu^{k'}}\} \bigcup \{C_{-5\mu^{k'}}\}$, *for* $0 \le k \le e-1, 0 \le k^{'} \le \frac{e}{2} - 1$.

Lemma 6.4. *Assume that* $q \equiv 2$ *or* $3 \pmod 5$. *For the q-cyclotomic cosets, one of the following holds.*

(1) If $4 \mid f$. *Let* $f = 4t$, *then*

(i) when t is even, we have that

$$C_0^* = C_0,\ C_\ell^* = C_\ell,\ C_{\mu^{k''}}^* = C_{-\mu^{k''}},\ C_{5\mu^k}^* = C_{5\mu^k},$$

where $\{C_{\mu^{k'}}\} = \{C_{\mu^{k''}}\} \bigcup \{C_{-\mu^{k''}}\}$, *for* $0 \le k \le e-1$, $0 \le k^{''} \le 2e-1$ *and* $0 \le k^{'} \le 4e-1$.

(ii) If t is odd, we have that

$$C_0^* = C_0,\ C_\ell^* = C_\ell,\ C_{\mu^{k'}}^* = C_{\mu^{k'}},\ C_{5\mu^k}^* = C_{5\mu^k},$$

where $0 \le k \le e-1$, $0 \le k^{'} \le 4e-1$.

(2) If $2 \mid f$ *but* $4 \nmid f$, *then*

$$C_0^* = C_0,\ C_\ell^* = C_\ell,\ C_{\mu^k}^* = C_{-\mu^k},\ C_{5\mu^k}^* = B_{5\mu^k},$$

where $\{C_{\mu^{k'}}\} = \{C_{\mu^k}\} \bigcup \{C_{-\mu^k}\}$, *for* $0 \le k \le e-1$, $0 \le k^{'} \le 2e-1$.

(3) If f is odd, then

$$C_0^* = C_0,\ C_\ell^* = C_\ell,\ C_{\mu^{k'}}^* = C_{-\mu^{k'}},\ C_{5\mu^{k'}}^* = C_{-5\mu^{k'}},$$

where $\{C_{\mu^k}\} = \{C_{\mu^{k'}}\} \bigcup \{C_{-\mu^{k'}}\}$, $\{C_{5\mu^k}\} = \{C_{5\mu^{k'}}\} \bigcup \{C_{-5\mu^{k'}}\}$, *for* $0 \le k^{'} \le \frac{e}{2} - 1$, $0 \le k \le e-1$.

From the above lemmas, we give all the self-dual cyclic codes of length $5 \cdot 2^s \ell$ over $\mathbb{F}_{2^m}$ and their enumeration in the following theorems.

Theorem 6.6. *Let $q \equiv 1 \pmod 5$, then one of the following holds.*

(1) If $f = \mathrm{ord}_\ell(q)$ is even, there exist $(2^s+1)^{2+2e}$ self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$, which are given by

$$\Big((x-1)^{2^{s-1}} C_\ell(x)^{\varepsilon_1} C_{-\ell}(x)^{2^s-\varepsilon_1} C_{2\ell}(x)^{\varepsilon_2} C_{-2\ell}(x)^{2^s-\varepsilon_2} \\ \times \prod_{k=0}^{e-1} C_{\mu^k}(x)^{\tau_k} C_{-\mu^k}(x)^{2^s-\tau_k} C_{2\mu^k}(x)^{\rho_k} C_{-2\mu^k}(x)^{2^s-\rho_k} C_{5\mu^k}(x)^{2^{s-1}}\Big),$$

where $0 \le \varepsilon_1, \varepsilon_2, \tau_k, \rho_k \le 2^s$, for any $0 \le k \le e-1$.

(2) If $f = \mathrm{ord}_\ell(q)$ is odd, there exist $(2^s+1)^{2+\frac{5e}{2}}$ self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$, which are given by

$$\Big((x-1)^{2^{s-1}} C_\ell(x)^{\varepsilon_1} C_{-\ell}(x)^{2^s-\varepsilon_1} C_{2\ell}(x)^{\varepsilon_2} C_{-2\ell}(x)^{2^s-\varepsilon_2} \\ \cdot \prod_{k=0}^{e-1} C_{\mu^k}(x)^{\tau_k} C_{-\mu^k}(x)^{2^s-\tau_k} C_{2\mu^k}(x)^{\rho_k} C_{-2\mu^k}(x)^{2^s-\rho_k} \prod_{k'=0}^{\frac{e}{2}-1} C_{5\mu^{k'}}(x)^{\iota_{k'}} C_{-5\mu^{k'}}(x)^{2^s-\iota_{k'}}\Big),$$

where $0 \le \varepsilon_1, \varepsilon_2, \tau_k, \rho_k, \iota_{k'} \le 2^s$, for any $0 \le k \le e-1$ and any $0 \le k' \le \frac{e}{2}-1$.

Proof.

(1) By Lemma 6.2, any self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$ has the form of

$$\Big((x-1)^{2^{s-1}} C_\ell(x)^{\varepsilon_1} C_{-\ell}(x)^{2^s-\varepsilon_1} C_{2\ell}(x)^{\varepsilon_2} C_{-2\ell}(x)^{2^s-\varepsilon_2} \\ \times \prod_{k=0}^{e-1} C_{\mu^k}(x)^{\tau_k} C_{-\mu^k}(x)^{2^s-\tau_k} C_{2\mu^k}(x)^{\rho_k} C_{-2\mu^k}(x)^{2^s-\rho_k} C_{5\mu^k}(x)^{2^{s-1}}\Big),$$

where $0 \le \varepsilon_1, \varepsilon_2, \tau_k, \rho_k \le 2^s$, for any $0 \le k \le e-1$. Since each of $\varepsilon_1, \varepsilon_2$ and τ_k, ρ_k, $0 \le k \le e-1$, has 2^s+1 possible values, we have in total $(2^s+1)^{2+2e}$ self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$.

(2) By Lemma 6.2, any self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$ has the form of

$$\Big((x-1)^{2^{s-1}} C_\ell(x)^{\varepsilon_1} C_{-\ell}(x)^{2^s-\varepsilon_1} C_{2\ell}(x)^{\varepsilon_2} C_{-2\ell}(x)^{2^s-\varepsilon_2} \\ \cdot \prod_{k=0}^{e-1} C_{\mu g^k}(x)^{\tau_k} C_{-\mu^k}(x)^{2^s-\tau_k} C_{2\mu^k}(x)^{\rho_k} C_{-2\mu^k}(x)^{2^s-\rho_k} \prod_{k'=0}^{\frac{e}{2}-1} C_{5\mu^{k'}}(x)^{\iota_{k'}} C_{-5\mu^{k'}}(x)^{2^s-\iota_{k'}}\Big),$$

where $0 \le \varepsilon_1, \varepsilon_2, \tau_k, \rho_k, \iota_{k'} \le 2^s$, for any $0 \le k \le e-1$ and any $0 \le k' \le \frac{e}{2}-1$. Each of $\varepsilon_1, \varepsilon_2$, $\tau_k, \rho_k, 0 \le k \le e-1$, and $\iota_{k'}$, $0 \le k' \le \frac{e}{2}-1$, has 2^s+1 possible values, we have in total $(2^s+1)^{2+\frac{5e}{2}}$ self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$. □

The proofs of theorems for the rest of cases are similar, and we will give them without proofs.

Theorem 6.7. *Let $q \equiv 4 \pmod 5$, then one of the following holds.*

(1) If $f = 2t$ is even, then

(i) when t is even, there exist $(2^s + 1)^{2e}$ self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$, which are given by

$$\left((x-1)^{2^{s-1}} C_\ell(x)^{2^{s-1}} C_{2\ell}(x)^{2^{s-1}} \prod_{k=0}^{e-1} C_{\mu^k}(x)^{\tau_k} C_{-\mu^k}(x)^{2^s-\tau_k} C_{2g^k}(x)^{\rho_k} C_{-2g^k}(x)^{2^s-\rho_k} C_{5g^k}(x)^{2^{s-1}}\right),$$

where $0 \le \tau_k, \rho_k \le 2^s$, for any $0 \le k \le e-1$.

(ii) when t is odd, there exists only one self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$, which is given by

$$\left((x-1)^{2^{s-1}} C_\ell(x)^{2^{s-1}} C_{2\ell}(x)^{2^{s-1}} \prod_{k'=0}^{2e-1} C_{\mu^{k'}}(x)^{2^{s-1}} C_{2\mu^{k'}}(x)^{2^{s-1}} \prod_{k=0}^{e-1} C_{5\mu^k}(x)^{2^{s-1}}\right).$$

(2) If f is odd, thenthere exist $(2^s + 1)^{3e/2}$ self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$, which are given by

$$\Big((x-1)^{2^{s-1}} C_\ell(x)^{2^{s-1}} C_{2\ell}(x)^{2^{s-1}}$$
$$\left.\times \prod_{k'=0}^{e/2-1} C_{\mu^{k'}}(x)^{\tau_{k'}} C_{-\mu^{k'}}(x)^{2^s-\tau_{k'}} C_{2\mu^{k'}}(x)^{\rho_{k'}} C_{-2\mu^{k'}}(x)^{2^s-\rho_{k'}} C_{5\mu^{k'}}(x)^{\iota_{k'}} C_{-5\mu^{k'}}(x)^{2^s-\iota_{k'}}\right).$$

Theorem 6.8. *Let $q \equiv 2$ or $3 \pmod 5$, then one of the following holds.*

(1) If $4 \mid f$. Let $f = 4t$, then

(i) when t is even, there exist $(2^s + 1)^{2e}$ self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$, which are given by

$$\left((x-1)^{2^{s-1}} C_\ell(x)^{2^{s-1}} \prod_{k''=0}^{2e-1} C_{\mu^k}(x)^{\tau_{k''}} C_{-\mu^{k''}}(x)^{2^s-\tau_{k''}} \prod_{k=0}^{e-1} C_{5\mu^k}(x)^{2^{s-1}}\right),$$

where $0 \le \tau_{k''} \le 2^s$, for any $0 \le k'' \le 2e-1$.

(ii) when t is odd, there exists only one self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$, which is given by

$$\left((x-1)^{2^{s-1}} C_\ell(x)^{2^{s-1}} \prod_{k'=0}^{4e-1} C_{\mu^{k'}}(x)^{2^{s-1}} \prod_{k=0}^{e-1} C_{5\mu^k}(x)^{2^{s-1}}\right),$$

(2) If $2 \mid f$ but $4 \nmid f$, then there exist $(2^s + 1)^e$ self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$, which are given by

$$\left((x-1)^{2^{s-1}} C_\ell(x)^{2^{s-1}} \prod_{k=0}^{e-1} C_{\mu^k}(x)^{\tau_k} C_{-\mu^k}(x)^{2^s-\tau_k} C_{5\mu^k}(x)^{2^{s-1}}\right),$$

where $0 \le \tau_k \le 2^s$, for any $0 \le k \le e-1$.

(3) If f is odd, then there exist $(2^s + 1)^e$ self-dual cyclic codes of length $5 \cdot 2^s\ell$ over $\mathbb{F}_{2^m}$, which are given by

$$\left((x-1)^{2^{s-1}} C_\ell(x)^{2^{s-1}} \prod_{k'=0}^{\frac{e}{2}-1} C_{\mu^{k'}}(x)^{\tau_{k'}} C_{-\mu^{k'}}(x)^{2^s-\tau_{k'}} C_{5\mu^{k'}}(x)^{\iota_{k'}} C_{-5\mu^{k'}}(x)^{2^s-\iota_{k'}}\right),$$

where $0 \leq \tau_{k'}, \iota_{k'} \leq 2^s$, *for any* $0 \leq k^{'} \leq \frac{e}{2} - 1$.

Acknowledgments

The first author was supported by the Yuyou Team Support Program of North China University of Technology (No. 107051360019XN137/007) and Yujie Talent Project of North China University of Technology(No. 107051360022XN735).

Conflict of interest

The authors declare no conflict of interest.

References

1. G. Bakshi, M. Raka, A class of constacyclic codes over a finite field, *Finite Fields Th. Appl.*, **18** (2012), 362–377. http://dx.doi.org/10.1016/j.ffa.2011.09.005
2. A. Batoul, K. Guenda, T. Aaron Gulliver, On repeated-root constacyclic codes of length $2^a mp^r$ over finite field, arXiv:1505.00356v1.
3. E. Berlekamp, *Algebraic coding theory*, New York: McGraw-Hill Book Company, 1968.
4. G. Castagnoli, J. Massey, P. Schoeller, N. von Seemann, On repeated-root cyclic codes, *IEEE T. Inform. Theory*, **37** (1991), 337–342. http://dx.doi.org/10.1109/18.75249
5. B. Chen, H. Dinh, H. Liu, Repeated-root constacyclic codes of length ℓp^s and their duals, *Discrete Appl. Math.*, **177** (2014), 60–70. http://dx.doi.org/10.1016/j.dam.2014.05.046
6. B. Chen, H. Dinh, H. Liu, Repeated-root constacyclic codes of length $2\ell^m p^n$, *Finite Fields Th. Appl.*, **33** (2015), 137–159. http://dx.doi.org/10.1016/j.ffa.2014.11.006
7. B. Chen, Y. Fan, L. Lin, H. Liu, Constacyclic codes over finite fields, *Finite Fields Th. Appl.*, **18** (2012), 1217–1231. http://dx.doi.org/10.1016/j.ffa.2012.10.001
8. H. Dinh, Repeated-root constacyclic codes of length $2p^s$, *Finite Fields Th. Appl.*, **18** (2012), 133–143. http://dx.doi.org/10.1016/j.ff a.2011.07.003
9. H. Dinh, Structure of repeated-root constacyclic codes of length $3p^s$ and their duals, *Discrete Math.*, **313** (2013), 983–991. http://dx.doi.org/10.1016/j.disc.2013.01.024
10. H. Dinh, On repeated-root constacyclic codes of length $4p^s$, *Asian-Eur. J. Math.*, **6** (2013), 1350020. http://dx.doi.org/10.1142/S1793557113500204
11. H. Dinh, Repeated-root cyclic and negacyclic codes of length $6p^s$, In: *Ring theory and its applications*, New York: Contemporary Mathematics, 2014, 69–87. http://dx.doi.org/10.1090/conm/609/12150
12. G. Hardy, E. Wright, *An introduction to the theory of numbers*, 5 Eds., Oxford: Clarendon Press, 1984.
13. J. Lint, Repeated-root cyclic codes, *IEEE T. Inform. Theory*, **37** (1991), 343–345. http://dx.doi.org/10.1109/18.75250

14. L. Liu, L. Li, X. Kai, S. Zhu, Reapeated-root constacylic codes of length $3\ell p^s$ and their dual codes, *Finite Fields Th. Appl.*, **42** (2016), 269–295. http://dx.doi.org/10.1016/j.ffa.2016.08.005

15. L. Liu, L. Li, L. Wang, S. Zhu, Reapeated-root Constacylic Codes of Length $n\ell p^s$, *Discrete Math.*, **340** (2017), 2250–2261. http://dx.doi.org/10.1016/j.disc.2017.04.018

16. A. Sharma, Repeated-root constacyclic codes of length $\ell^t p^s$ and their dual codes, *Cryptogr. Commun.*, **7** (2015), 229–255. http://dx.doi.org/10.1007/s12095-014-0106-5

17. A. Sharma, S. Rani, Repeated-root constacyclic codes of length $4\ell^m p^n$, *Finite Fields Th. Appl.*, **40** (2016), 163–200. http://dx.doi.org/10.1016/j.ffa.2016.04.001

18. Z. Wan, *Lectures on finite fields and galois rings*, New York: World Scientific, 2011. http://dx.doi.org/10.1142/8250

19. Y. Wu, Q. Yue, Factorizations of binomial polynomials and enumerations of LCD and self-dual constacyclic codes, *IEEE T. Inform. Theory*, **65** (2019), 1740–1751. http://dx.doi.org/10.1109/TIT.2018.2864200

20. Y. Wu, Q. Yue, S. Fan, Further factorization of $x^n - 1$ over a finite field, *Finite Fields Th. Appl.*, **54** (2018), 197–215. http://dx.doi.org/10.1016/j.ffa.2018.07.007

AIMS Press